Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

APT Analyse mit Splunk

Whitepaper

10. Juli 2014

Quelldokument:	compass_security_schweiz_whitepaper_apt_network_analysis_w_splunk_v1.1.docx
Version:	v1.1
Autor:	Lukas Reschke
Auslieferungsdatum:	10. Juli 2014
Klassifikation:	ÖFFENTLICH

Inhaltsverzeichnis

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

1 Übersicht

1.1 Audienz

Dieses Whitepaper richtet sich an die Mitarbeiter der Compass Security Schweiz AG und sonstige Interessierte. Das vorliegende Dokument ist um eine allgemeinverständliche Sprache bemüht.

1.2 Versionskontrolle

Version	Datum	Änderungen	Autor
0.1	11.10.2013	Erstellung der Dokumentenstruktur	Lukas Reschke
0.5	25.03.2014	Dokumentation der Ergebnisse	Lukas Reschke
0.9	10.04.2014	Gramatikalische und inhaltliche Korrekturen	Lukas Reschke
1.0	11.04.2014	Auslieferung	Lukas Reschke
1.1	10.07.2014	Update	Lukas Reschke

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2 Einleitung

Kunden der Compass Security Schweiz AG werden vermehrt Opfer von APT (Advanced Persistent Threat [zu Deutsch etwa "fortgeschrittene, andauernde Bedrohung"]) Angriffen. Unter diese Bezeichnung fallen komplexe, zielgerichtete und äusserst effektive Angriffe auf kritische und zuweilen gar unternehmenswichtige Computersysteme.

Die Analyse von potentiell infiltrierten Netzen und Systemen gestaltet sich jedoch als enorm aufwändig, da Unmengen von Datensätzen und Logs ausgewertet werden müssen. Im Fokus dieses Whitepapers steht daher die Analyse von APT mittels Splunk, einer spezialisierten Software zur Analyse von grossen Mengen maschinengenerierter Logdaten. Ebenfalls sollen alternative Wege zur Auswertung eruiert werden und ein Standardvorgehen für Fälle von APT entwickelt werden.

2.1 Begriffsdefinition

Der Begriff des Advanced Persistent Threats (im folgendem als APT abgekürzt) wurde massgeblich von der amerikanischen IT-Sicherheitsfirma Mandiant geprägt. In einem Bericht aus dem Jahr 2010 ging Mandiant auf die massiv gestiegene Anzahl von Angriffen auf kritische Zielgruppen wie z.B. Regierungsbehörden ein (Mandiant, 2010). Im Gegensatz zu früheren Angriffen, ist die Komplexität einiger Angriffe jedoch erstaunlich gross und erfordert die Ausnutzung von äusserst komplexen Angriffsvektoren. Selbst sogenannte Zero-Day-Exploits, ein IT-Fachbegriff für die Ausnutzung einer bis anhin unbekannten und darum besonders wertvollen Sicherheitslücke, wurden für diese Attacken genutzt.

Mittlerweile sind eine Vielzahl von Angriffen öffentlich dokumentiert. Ein Plural der Angriffe wird aber niemals aufgedeckt oder gar nicht erst an die Öffentlichkeit kommuniziert:

- Das iranische Atomprogramm wurde durch einen Angriff auf die Atomanlage "Natanz" nahezu lahmgelegt und um Jahre zurückversetzt. Diese Malware wurde als Stuxnet bekannt und besitzt selbst in weniger IT affinen Umkreisen durchaus an Bekanntheit. (Mandiant, 2010)
- RSA Security, ein amerikanischer Anbieter für weitverbreitete Sicherheitslösungen, wurde mittels eines nicht näher definierten APT Angriffes angegriffen.[1]
- Zahlreiche tibetische Oppositionelle und Exilregierungsmitglieder wurden mittels einer Spear-Phishing Attacke Opfer eines Cyberangriffes.[2]
- Das bekannteste Beispiel sind vermutlich die zahlreichen Abhörskandale der amerikanischen National Security Agency, welche erst durch Edward Snowden bekannt geworden sind.[3]

Um ein genaueres Verständnis zu erlangen, um was es sich bei "Advanced Persistent Threats" handelt, ist es lohnenswert, den Begriff von seinen Wortbestandteilen her zu erklären. Es ist jedoch eine begrenzende Prämisse, dass es keine einzige allgemeingültige Definition für "APT" gibt, viel mehr wird der Begriff oftmals auch kontextsensitiv angewendet.

Advanced: Angreifer hinter APT-Angriffen setzen üblicherweise auf enorm fortgeschrittene Angriffsmethoden. Dies beinhaltet die bereits genannten Zero-Day Attacken als auch Angriffszenarien, welche ohne enorme aussergewöhnlich grosse Anstrengungen nicht möglich sind (z.B. das Abhören von Glasfaserleitungen).

Persistent: Das Ziel eines APT ist es, möglichst lange unentdeckt aktiv zu sein und so langfristig Informationen an den Angreifer zu übermitteln oder Schadcode auszuführen.

Threat: Englisch für Bedrohung.

[1] Vgl. http://www.wired.com/beyond_the_beyond/2011/03/rsa-compromised-by-advanced-persistent-threat/
[2] Vgl. http://www.securelist.com/en/blog/208193616/New_MacOS_X_backdoor_variant_used_in_APT_attacks
[3] Vgl. http://heise.de/-2039019

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2.2 Angriffszenarien

Bei einem APT muss von einem komplett anderem und viel differenziertem Angriffszenario ausgegangen werden als bei alltäglichen Attacken. Vor allem muss aber davon ausgegangen werden, dass ein erfolgreicher Angriff zuerst – oder sogar gar nicht – bemerkt wird.

Die Compass Security Schweiz AG wurde bereits mehrmals in Fällen von mutmasslichen APT mit der Analyse beauftragt. Es hat sich nicht selten herausgestellt, dass der vermeintliche Angriff in dieser Form gar nicht stattfand. Dafür aber unter Umständen andere erfolgreiche Angriffe stattgefunden haben.

Das erschwert die Analyse eines potentiellen APT um einiges, denn der Analyst kann sich niemals sicher sein, ob überhaupt ein Angriff erfolgt ist oder ob es sich lediglich um eine – oftmals unbegründete – Befürchtung handelt. Daher muss die Analyse immer in der Vogelperspektive erfolgen. Es kann anfangs nicht Rücksicht auf einzelne Systeme genommen werden, sondern es muss das gesamte Netzwerk betrachtet werden. Dies ist bei Netzwerken mit mehreren zigtausenden Geräten aber auch die einzige Möglichkeit, in einer sinnvollen Zeit zu Ergebnissen zu gelangen.

Auch wenn ein APT für den Laien erstmals undetektierbar wirkt ist eine Erkennung durchaus möglich. Sind die Verbreitungswege eines APT doch genau identisch mit denen einer üblichen Schadsoftware.

- Verbreitung via Phishing
    - Phishing mag erstmal unattraktiv klingen, denkt man da doch zunächst an Mails mit mangelhafter Rechtschreibung. Doch ein professioneller Angriff kann äusserst erfolgreich sein. Welcher Angestellte würde denn nicht die nette Weihnachtskarte (mit hübschen USB Stick im Firmenlogo) der Geschäftsleitung benutzen?
- Verbreitung via Sicherheitslücken
    - Die Verbreitung über unbekannte Sicherheitslücken ist sicherlich der erfolgsversprechendste und unaufälligste Verbreitungsvektor. Besonders Regierungsbehörden nutzen dies, gibt es doch Unternehmen wie VUPEN[4], welche ihr Geld mit dem Verkauf von ausnutzbaren Sicherheitslücken an diverse Sicherheitsbehörden (unter anderem die NSA) verdienen.
- Verbreitung via Social Engineering
    - Beim "Social Engineering" wird versucht die Gutgläubigkeit von anderen Menschen auszunutzen. So wird der vermeintliche Elektriker eben mal schnell ins Gebäude gelassen, um den vermeintlichen Leistungsverlust auf Geheiss der Geschäftsleitung zu beheben. Im Gebäude selbst vollführt dieser dann den Angriff.
- Verbreitung via "Inside Jobs"
    - Oftmals werden ehemalige oder aktive Mitarbeiter verdächtigt, sogenannte Backdoors hinterlassen zu haben. Falls der mutmassliche Täter als System- oder gar Firewalladministrator eingestellt war oder ist, besitzt dieser ein fundiertes Wissen über die Infrastruktur und hat administrativen und möglicherweise sogar physikalischen Zugriff auf eine Vielzahl von Systemen. Dies ist ein sehr bedrohliches Szenario. Eine Analyse gestaltet sich in solchen Fällen als äusserst komplex.

Es ist wichtig, sich vor Augen zu halten, dass es so etwas wie absolut sichere und unknackbare Systeme nicht gibt und auch in näherer Zukunft nicht geben wird. Für einen Angreifer mit beinahe unlimitierten Ressourcen wird es immer Einfallstore geben, denn jedes System ist nur so stark, wie sein schwächstes Glied und das ist im Falle der Informationstechnik oftmals der Mensch.

[4] Vgl. http://www.vupen.com/english/services/lea-index.php

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Reaktive Massnahmen reichen beim Betrieb von kritischer Infrastruktur keineswegs aus. Um die bestmöglichste Sicherheit der eigenen Infrastruktur zu gewährleisten, ist es unerlässlich, auch auf proaktive Massnahmen wie regelmässige und professionell durchgeführte Penetrationtests zu setzen. Die Compass Security Schweiz AG berät eine Vielzahl von nationalen und internationalen Unternehmungen.

Trotz der zahlreichen und verschiedenen Angriffsvektoren, werden diese im Bereich der Informationssicherheit pragmatischerweise oftmals nur in zwei verschiedene Kategorien eingeteilt, den sogenannten direkten und indirekten Angriffsvektoren.

2.2.1 Direkte Angriffsvektoren

Bei direkten Angriffsvektoren handelt es sich um Attacken, bei welchem ein Angreifer direkt versucht, Zugriff auf interne Systeme zu erlangen. Dies kann zum Beispiel durch die Ausnutzung einer Sicherheitslücke in einem unzureichend gepatchten System erfolgen.

In Abbildung 1 ist ein solcher Angriff schematisch dargestellt. Solche Angriffe werden jedoch oft von einer Firewall abgeblockt oder die entsprechenden Systeme sind nur vom internen Netz aus erreichbar.

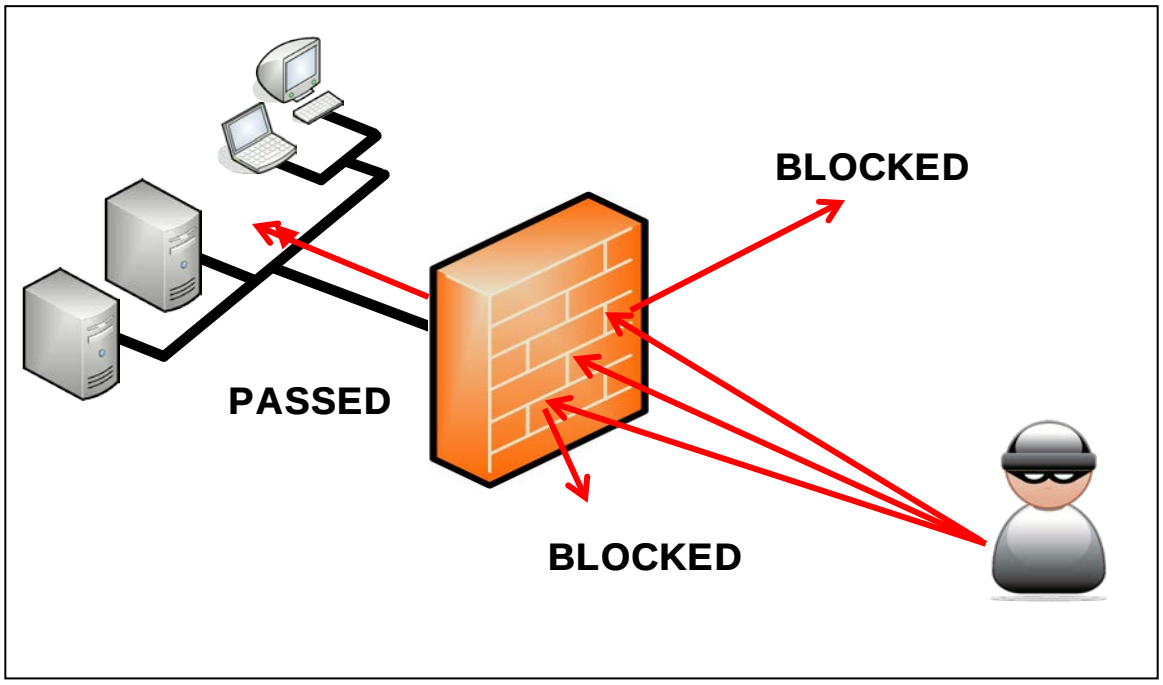


Abbildung 1 - "Direct Attack" Angriffsvektor (Quelle: Compass Security Schweiz AG)

Diese äusserst einfache Angriffsmethode setzt jedoch eine äusserst unzureichende Netzwerkonfiguration voraus. Durch die Segmentierung von Systemen in Netzen mit verschiedenen Vertraulichkeitsstufen sollte selbst ein erfolgreicher Angriff keine weiterreichenden Folgen haben.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2.2.2 Indirekte Angriffsvektoren

Indirekte Angriffsvektoren sind wesentlich differenzierter und bedürfen oft eines hohen Aufwands und eines beachtlichen Ausmasses an Kreativität, um Zugriff auf ein Netz zu erlangen. In Abbildung 2 wird so zum Beispiel ein Angriff visualisiert, welcher zuerst die privaten Geräte eines Mitarbeiters infiziert, um dann schlussendlich Zugriff auf die internen Systeme zu erlangen.

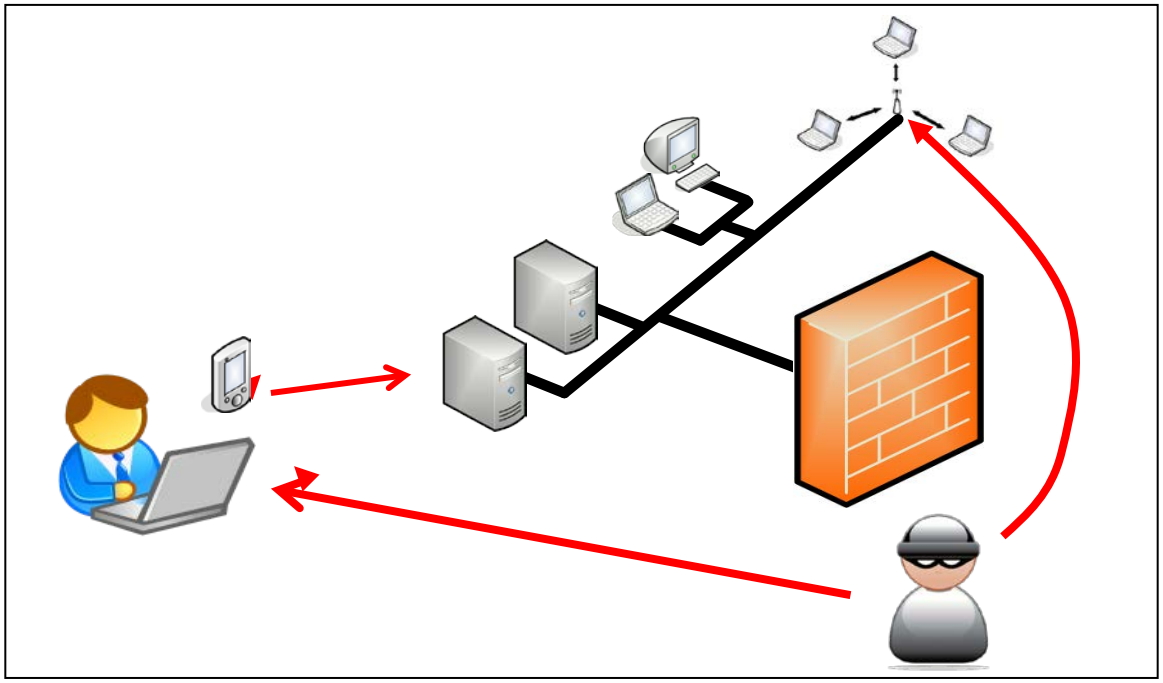


Abbildung 2 - "Indirect Attack" Angriffsvektor (Quelle: Compass Security Schweiz AG)

Durch die enorme Zunahme des BYOD-Trends ("Bring Your Own Device") bei welcher Mitarbeiter ihre eigenen Mobilgeräte (Laptops / Tablets / Smart Phones / etc...) in der Unternehmung nutzen dürfen, wird dieser Angriffsvektor immer lukrativer. Diese Geräte können oftmals nicht ausreichend zentral administriert werden und stellen daher unter Umständen ein erhebliches Sicherheitsrisiko für Unternehmungen dar.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2.3 APT-Charakteristiken

Die genauen Charakteristiken eines APT lassen sich aufgrund der Vielfalt von Angriffsmethoden nicht genau definieren. Dennoch will ich hier versuchen, eine grobe Definition zu erstellen:

- Ein APT hat eine spezifische Organisation – oftmals auch ohne finanziellen Hintergrund - als Ziel. Ein gewöhnlicher Angreifer ist normalerweise an wirtschaftlich lohnenswerteren Zielen interessiert.
- Ein APT ist langsam und methodisch, man könnte das Vorgehen fast als äusserst strategisch beschreiben. Der normale Angreifer nutzt jedoch üblicherweise jede noch so auffällige Gelegenheit aus, um Zugriff auf ein System zu erlangen.
- Ein APT greift auf spezielle und für diesen Fall massgeschneiderte Tools und Angriffsmethoden zurück. Der gewöhnliche Angreifer benutzt in den allermeisten Fällen lediglich gängige Tools und Programme.
- Ein APT versucht, das System derart zu infiltrieren, dass eine Entfernung fast unmöglich ist. Er wird anstreben, weitere interne Systeme zu befallen oder sich gar permanent in Dateien (z.B. Quellcode) einzunisten.

Eine gute Analogie zum realen Leben ist zum Beispiel ein Taschendiebstahl. Ein gewöhnlicher Dieb würde jede beliebige Tasche klauen, welche ihm in die Finger gerät. Es geht ihm nur um den kurzfristigen Gewinn.

Ein APT hätte sich hingegen das Ziel gesetzt, eine spezifische Tasche zu entwenden und kann sich zur Zielerreichung viel Zeit nehmen. Er wählt diesen Weg, weil der Angreifer weiss, dass diese besonders wertvolle Objekte beinhaltet.

Oftmals wird jedoch ein Faktor völlig ignoriert oder unterbewertet, nämlich die eigenen Mitarbeiter. Diese besitzen oftmals bereits Zugriff auf viele interne Systeme und können daher ohne einen Angriff Daten kopieren. Das Beispiel vom NSA Whistleblower Edward Snowden, welcher mittels kostenloser Crawlersoftware[5] einen enormen Teil des Datenbestandes der NSA kopiert hat, zeigt, wie wichtig die Erkennung von Anomalien auch in einem vermeintlich uninteressanten Unternehmensnetzwerk ist.

[5] Vgl. http://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

3 Forensisches Vorgehen

In Rahmen einer forensischen Analyse, bei der ein Anspruch auf gerichtsverwertbare und stichfeste Ergebnisse besteht, ist es äusserst wichtig, das Grundvorgehen in einem klar definierten und nachvollziehbaren Prozess darzustellen. Die Vorgehensweise basiert auf der Annahme, dass ein Angreifer immer noch Zugriff auf die potentiell kompromittierten Systeme besitzt. Das Ziel ist die Erkennung eines Angreifers, ohne das dieser davon erfährt.

Die Compass Security AG hat sich für die folgende Vorgehensweise entschieden:

Abbildung 3 - Forensisches Vorgehen bei der Compass Security Schweiz AG

Das Vorgehen basiert auf den folgenden fünf Phasen:

1. Health Check Phase
    - In dieser Phase wird analysiert, ob die notwendigen Logdaten vorhanden sind und ob diese bereits offensichtliche Informationen über den Angreifer enthalten.
2. Preparation
    - Im Anschluss an die Analyse der Logqualität stellt sich möglicherweise heraus, dass einige Anpassungen vorgenommen werden müssen, um mehr Details zu erhalten.
3. Record Events
    - Nachdem alles dermassen aufgesetzt ist, dass eine Analyse Chancen auf Erfolg verspricht, muss über einen längeren Zeitraum die Aufzeichnung der Daten erfolgen. Ein Aufzeichnungszeitraum von mindestens einer Woche ist sinnvoll, um genug Daten für eine Analyse zu erhalten.
4. Analyze Events
    - In dieser Phase werden die gewonnenen Daten vom Analysten auf legitimen respektive illegitimen Datenverkehr untersucht.
5. Targeted Analysis
    - Schlussendlich sollte herauskommen, welches Hostsystem für den fragwürdigen Datenverkehr zuständig ist und das betroffene System kann eigenständig untersucht werden. Auf die abschliessende Analyse eines einzelnen Systems kann nicht im Rahmen dieses Dokumentes eingegangen werden, weil dies den Rahmen sprengen würde.

Auf die einzelnen Phasen wird in den nachfolgenden Kapiteln näher eingegangen.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

3.1 Phase 1: Health Check

3.1.1 Netzwerktopologie

Damit eine Analyse erfolgreich sein kann, ist es zwingend notwendig, dass das betroffene Netzwerk so aufgesetzt ist, dass genügend aussagekräftige Logdaten gewonnen werden können.

Der Sicherheitsforscher Samy Kamkar hat die häufig massiven Unterschiede zwischen Vorstellung und Realität äusserst passend visualisiert:

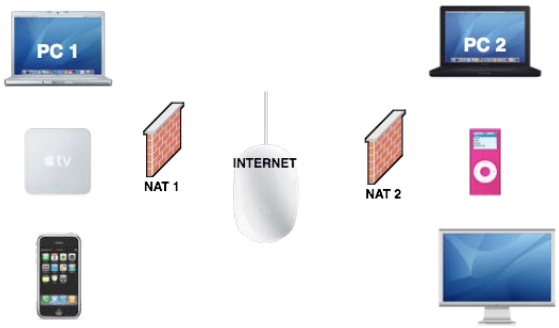


Abbildung 4 - Vorstellung eines Netzwerkes (Quelle: (Kamkar, 2012))

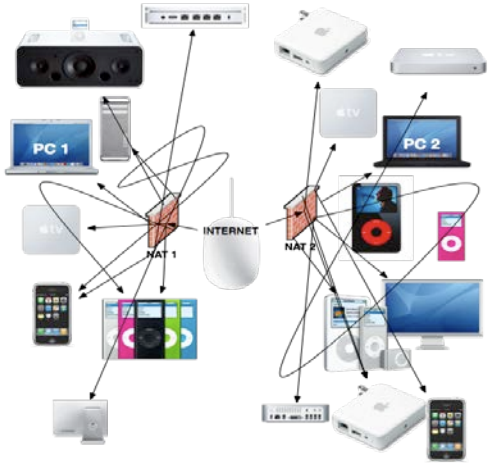


Abbildung 5 - Reale Abbildung eines Netzwerkes (Quelle: (Kamkar, 2012))

Auch wenn sich diese Abbildung auf ein typisches Netzwerk eines Privatnutzers bezieht, ist dies durchaus auch von Relevanz für Unternehmungen. Zwar besteht in solchen Fällen oft eine Netzwerktopologie, aber diese sind nicht immer auf dem aktuellen Stand oder die Anforderungen an ein analysierbares Netzwerk sind nicht erfüllt.

Um möglichst grosse Chancen auf eine potentiell erfolgreiche Analyse zu besitzen, ist es hilfreich, wenn die folgenden Bedingungen erfüllt sind:

- DNS Anfragen dürfen nur über einen internen Resolver erfolgen und müssen geloggt werden.
- HTTP(S) Datenverkehr muss über einen zentralen Proxy erfolgen. Verschlüsselter Verkehr sollte aufgebrochen werden. Die Daten müssen geloggt werden.
- Die Endgeräte sollen nur in der Lage sein, Verbindungen aufzubauen, welche zwingend notwendig sind. Unnötige Protokolle (z.B. FTP) sollten in der Firewall blockiert werden.
- Verbindungen durch die Firewall sollten geloggt werden.
- Dateizugriffe auf Netzwerklaufwerke sollten zentral geregelt sein und dokumentiert werden.

Empfehlungen wie einzelne Komponenten bezüglich der Logdaten konfiguriert werden sollten, sind im Kapitel 7 auf Seite 50 zu finden.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

3.1.2 Zentrale Logverwaltung

Nach einer erfolgreichen Infiltration eines Computernetzwerkes ist es für einen Angreifer oftmals das erste Ziel, die Spuren zu verwischen, um möglichst lange von diesem Gerät aus operieren zu können.

In vielen Umgebungen wird ein Angreifer sogar oftmals in der Lage sein, einen Grossteil oder sogar alle Spuren zu vernichten. Zwar gehört das Logging mittlerweile bei einem Server zum guten Ton, jedoch werden diese oftmals nur lokal auf den betroffenen Servern gespeichert und können daher vom Angreifer beliebig verändert werden.

Das führt auch zu einem anderen Problem: nämlich der Vertrauenswürdigkeit von Logs. Logs werden oft als unfehlbares Mittel zur Beweissicherung angesehen. Diese Fehleinschätzung kann aber zu fatalen Fehlurteilen führen. Ist doch ein Angreifer sogar oftmals in der Lage, falsche Spuren zu legen, damit jemand anderes in Verdacht gerät, diesen Angriff durchgeführt zu haben.

Ein Mittel, um eine hohe Integrität von Logfiles zu garantieren sind sogenannte Remote Syslog Services wie unter anderem rsyslog[6] oder syslog-ng[7]. Diese Services dienen zur zentralen Ablage von Logdaten.

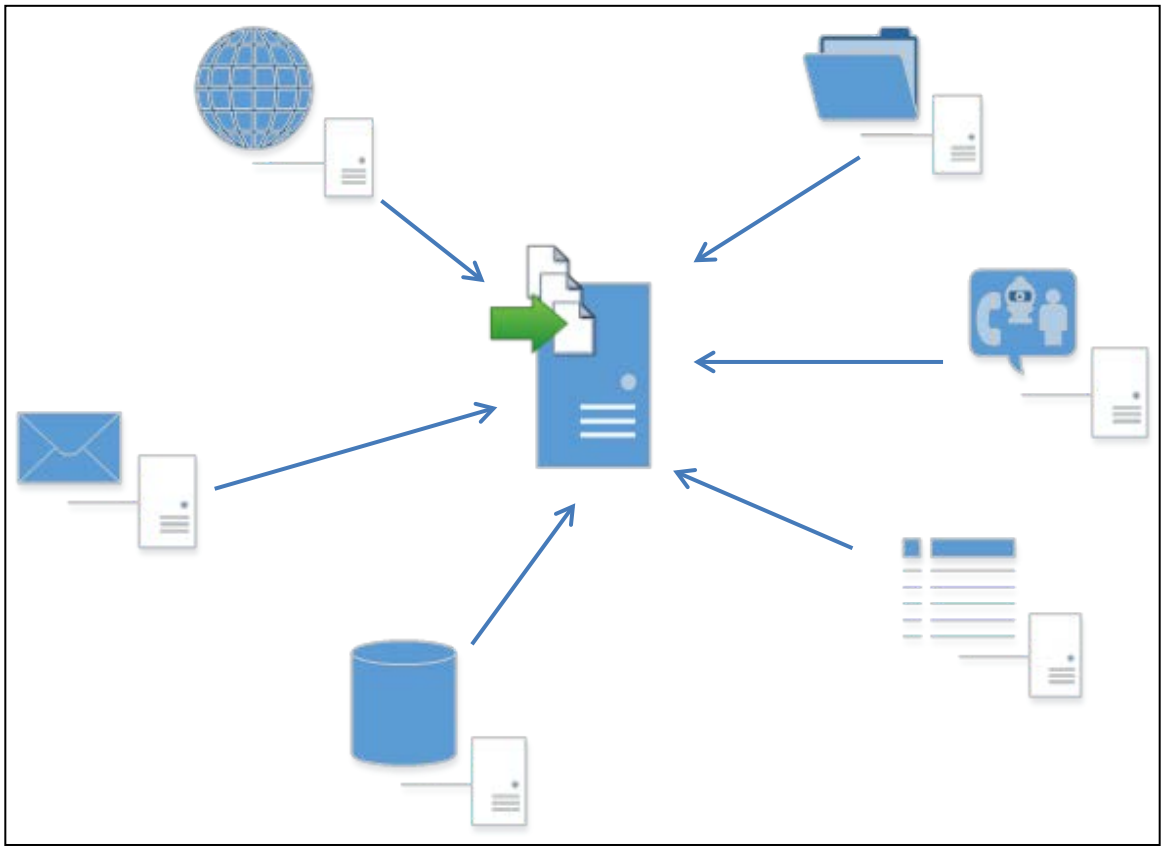


Abbildung 6 - Remote Syslogging

Aber selbst solche Services können die totale Integrität eines Logs nicht garantieren. Ein Angreifer kann immer noch alle Logeinträge *nach* dem erfolgreichen Angriff manipulieren, die Logeinträge davor sind jedoch

[6] http://www.rsyslog.com/
[7] http://www.balabit.com/network-security/syslog-ng/

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

bereits auf dem Logserver und können nicht mehr verändert werden. Dies führt dazu, dass zumindest die Angriffsversuche und das Deaktivieren des Loggingservices in den Logs aufgeführt sind.

Leider hat Compass Security die Erfahrung gemacht, dass solche Services in vielen Infrastrukturen nicht oder nur bei wenigen Servern eingesetzt werden. Wenn ein Angreifer in der Lage ist, die Logs verändern zu können ist eine Analyse deutlich erschwert.

3.2 Phase 2: Preparation

Um an verwertbare und sinnvolle Logs zu gelangen, ist es zunächst notwendig sicherzustellen, welche Geräte potentielle bösartige Aktionen aufgezeichnet haben könnten. Wie diese Logs am besten exportiert werden können, wird für eine Auswahl von gängigen Geräten und Applikationen im Kapitel 7 auf Seite 50 dokumentiert.

Um festzustellen, welche Komponenten potential auswertbar sind, ist es zunächst notwendig, ein Grundverständnis über die wichtigsten Services zu erhalten. In der nachfolgenden Tabelle wird auf die unterschiedlichen Services eingegangen und wie diese allfällig verwertbar sind.

Service	Was macht der Service?	Wie ist das verwertbar?
DHCP Server	Dieser weist einem Gerät bei Nachfrage eine IP Adresse aus einem Adresspool zu.	Es kann unter Umständen festgestellt werden, ob sich ein neues Gerät in das Netz angemeldet hat. Dafür ist es allerdings erforderlich, dass die Unternehmung über eine Liste mit allen benutzten MAC Adressen verfügt.
Directory Server (AD / LDAP)	Er wird zur Benutzerverwaltung eingesetzt. Dies ist in grösseren Betrieben unerlässlich, um eine effiziente Verwaltung zu garantieren.	Es kann unter Umständen festgestellt werden, ob ein Benutzer zu einer bestimmten Zeit angemeldet war oder sich für Services authentifiziert hat.
DNS Server	Er ist verantwortlich für die Auflösung von Domainnamen in IP Adressen. z.B. `csnc.ch → 212.254.246.115`	DNS wird oft als beliebtes Mittel für DNS Tunneling (Covert Channel) genutzt. Auch lassen sich Anomalitäten im DNS Verkehr einzelner Hosts feststellen.
Mail Server	Dient der Auslieferung von E-Mails an interne und externe Nutzer.	Es kann festgestellt werden, ob interne Firmendaten nach aussen kommuniziert wurden. Ebenfalls können E-Mails als Kommunikationskanal für Malware genutzt werden. Mittels einer statistischen Analyse lässt sich feststellen, ob ein Nutzer enorm grosse Mengen an Mails

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Service	Was macht der Service?	Wie ist das verwertbar?
		empfängt und versendet.
Perimeter Firewall	Steht als Segmentierungselement zwischen zwei Zonen.	Man kann Verbindungen zwischen verschiedenen Netzwerkzonen loggen. So kann z.B. festgestellt werden, welches Gerät Verbindungen in ein internes Managementnetz aufgebaut hat.
Proxy Server	Dienen als Segmentierungselement zwischen Absender und Empfänger. Sie sind oftmals die einzige Schnittstelle nach draussen.	Aufgrund der Proxylogs können Unregelmässigkeiten im Verkehr ins Internet festgestellt werden. (z.B. Malware Beacons)
Spiegelports auf zentralen Switches	Spiegeln den ein- und ausgehenden Netzwerkverkehr von einem LAN Port auf ein anderes.	Durch eine Analyse des Netzwerkverkehres lassen sich weitreichende Schlussfolgerungen auf die Tätigkeiten des Nutzers ziehen. Diese sogenannte "Deep Packet Inspection" ist rechtlich jedoch äusserst bedenklich.

Tabelle 1 - Auswertbare Netzwerkkomponenten

Diese nicht abschliessende Auflistung der verwertbaren Logdatenquellen zeigt, dass während einer Analyse enorme Mengen an Daten zu verarbeiten sind. Es ist daher enorm schwierig, gutartige und bösartige Systeme zu erkennen.

Anleitungen und Anregungen für eine angemessene Konfiguration der Logs für ausgewählte Applikationen sind im Kapitel 7 zu finden. In jedem Fall geloggt werden sollte:

- Typ der Aktion
- Quelladresse
- Zieladresse
- Benutzername
- Zeitstempel

3.3 Phase 3: Record Events

Die Logdaten werden dann gesammelt und für eine spätere Analyse gespeichert. Das Speichern von Daten ist grundsätzlich ein Langzeitunterfangen, denn es werden für eine möglichst aufschlussreiche Analyse möglichst viele Datensätze benötigt.

Es ist nicht zwingend notwendig, dass diese Phase komplett abgeschlossen ist, bevor mit der Analyse fortgefahren werden kann. Die Loganalyse kann grundsätzlich gleichzeitig erfolgen, um ein zeitsparendes Vorgehen zu ermöglichen

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

3.4 Phase 4: Analyze Events

Alle vorherigen Phasen hatten die grobe Analyse der Netzwerkinfrastruktur als Ziel. Das Ziel dieser Phase ist die Unterscheidung zwischen bösartigen und gutartigen Ereignissen in den Logdaten.

Die Unterscheidung, ob ein Ereignis gut- oder bösartig ist, ist äusserst zeitaufwändig. Der Analyst muss den Datenverkehr, der nicht definitiv automatisiert als gut oder bösartig eingestuft werden kann, eigenständig verifizieren. Dazu muss der Analyst anhand von Informationen, die der Kunde bereitgestellt hat, das Ereignis beurteilen. Hierfür ist eine "Kommunikationsmatrix" sehr hilfreich. Diese kann dem Analysten helfen zu beurteilen, ob Verbindungen legitimer Natur sind.

Ebenfalls sucht der Analyst nach schädlichen Aktivitäten wie zum Beispiel Verbindungen zu bösartigen Websiten. In Zusammenarbeit mit dem Kunden wird entschieden, auf welche Systeme genauer eingegangen werden soll.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4 Erkennungsmethodiken

Zur Erkennung von APT gibt es aus verständlichen Gründen kein Standardvorgehen im eigentlichen Sinn, welches eine Lösung für alle Probleme verspricht. Es gibt zwar Programme, welche versprechen, Angriffe frühzeitig zu erkennen und auch abzuwehren. Doch auch diese stellen keineswegs eine perfekte und umungehbare Lösung zur Absicherung eines Unternehmensnetzwerkes dar.

Sebastian Strobel hat im Artikel "Technische Ansätze zum Schutz vor APTs" in der Computerfachzeitschrift iX eine recht übersichtliche Grafik erarbeitet (vgl. Abbildung 7) welche die unterschiedlichen Erkennungsmethoden visualisiert:

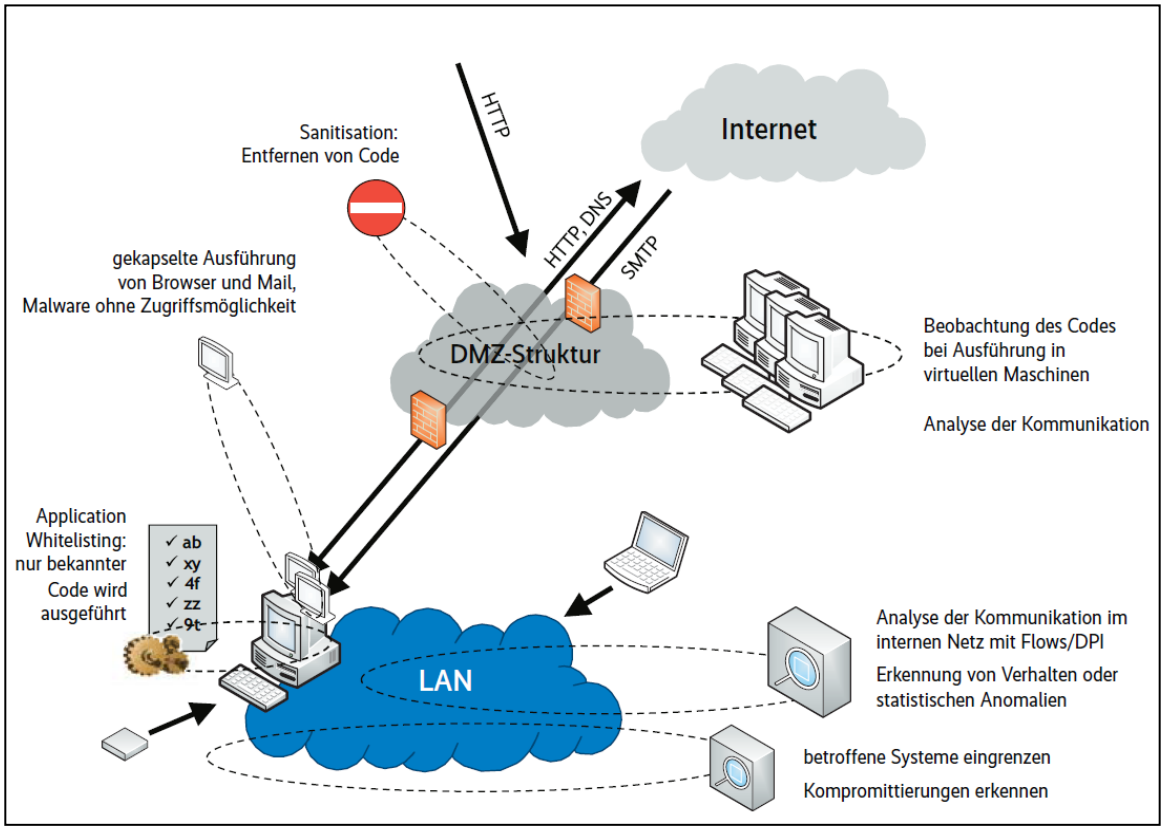


Abbildung 7 - Die verschiedenen Ansätze der APT-Bekämpfung setzen an unterschiedlichen Angriffsvektoren ein. (Quelle: (Strobel, 2014))

Im Folgenden wird etwas detaillierter auf die einzelnen Ansatzpunkte eingegangen und die Vor- und Nachteile der Methoden dargestellt. Eine Kurzübersicht befindet sich in 0 auf Seite 21. Aufgrund des beschränkten Fokuses dieses Whitepapers, wird im späteren Verlauf nur auf die verhaltensbasierende Erkennung respektive der Erkennung von statistischen Anomalien eingegangen.

Da Compass generell von Empfehlungen für einzelne Produkte absieht, wird im Folgenden nur auf die allgemeinen Eigenschaften und Funktionen eingegangen und keine Rücksicht auf einzelnen Produkte genommen.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.1 Sanitisation: Entfernung von Code

Bei der Sanitisierung, also der Veränderung oder Entfernung von Code, steht nicht die Erkennung im Vordergrund, sondern primär die Verhinderung von Angriffen.

So gibt es zum Beispiel Mail- und Webgateways, welche versuchen, jegliche übertragenene Dateien in ein anderes Format zu konvertieren. So werden zum Beispiel Word Dateien in ein PDF umgewandelt oder Bilder in ein komplettes anderes Bildformat konvertiert.

Dies hat zur Folge, dass bösartige Inhalte während der Konvertierung aus den ausgelieferten Dateien entfernt werden. Diese Lösung hat aber auch die Konsequenz, dass der Dateiaustausch mit externen Parteien stark erschwert wird und für vertrauenswürdige Drittparteien ein eigener Kommunikationskanal eingerichtet werden muss. Ebenfalls existiert nicht für jedes Dateiformat ein nutzbares Pendant, so dass dieser Ansatz nur für gängige Dateitypen möglich ist.

4.2 Beobachtung des Codes bei Ausführung in virtuellen Maschinen

Diese Methode verspricht durch eine verhaltensbasierte Analyse bei der Ausführung der Datei zu erkennen, ob die Datei bösartig oder gutartig ist. Dieser Ansatz ist durchaus sehr interessant, ist aber aus verschiedenen Gründen nicht immer sinnvoll:

- Eine initiale Infizierung lässt sich damit oftmals nicht zuverlässig vermeiden. Aus Zeitgründen wird während der ersten Analyse des Programmes, dieses bereits nach einer kurzen Zeitspanne an den Benutzer ausgeliefert. Eine Verzögerung des Versands um mehrere Stunden ist in einer produktiven Umgebung oftmals nicht wünschenswert.
- Eine Malware kann durchaus auch einige Zeit (z.B. einen ganzen Tag) keine Aktionen ausführen, bevor der bösartige Code zeitverzögert ausgeführt wird. Wenn die Analysen oftmals nicht derart lange Zeitspannen umfassen, wird solche Malware nicht erkannt.
- Die Heuristik, ob ein Programm gutartig oder bösartig ist, basiert immer auf bekannten Verhaltensmustern. Eine neuartige Attacke würde durch solch einen Schutzmechanismus nicht erkannt werden.

Der vermutlich grösste Vorteil derartiger Lösungen ist es, dass im Falle einer grossflächigen Infektion, die Chance gross ist, dass diese automatisiert erkannt werden kann.

4.3 Gekapselte Ausführung von Browser und Mail

Bei einer sogenannten "gekapselten Ausführung" von Programmen laufen diese nicht auf dem gleichen Betriebssystem. Sollte eines der Programme nun durch einen Angreifer erfolgreich kompromittiert worden sein, so kann dieser nicht auf die Daten des anderen Programmes zugreifen.

Grundsätzlich ist es möglich, dies durch die folgenden Vorgehensweisen umzusetzen:

- Einsatz von verschiedenen virtuellen Systemen auf einem Rechner
    - Verschiedene virtuelle Betriebssysteme laufen auf einem Rechner und besitzen keine Möglichkeit, untereinander zu kommunizieren. Kritische Programme werden jeweils in einer anderen virtuellen Maschine eingesetzt.
- Einsatz von "Remote-Controlled Browsers System" (ReCoBS)
    - Die Endnutzer sind komplett vom Internet abgekoppelt und können nur über den Remote Browser mit dem Internet interagieren.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Vor allem der Einsatz von ReCoBS gewinnt immer mehr an Attraktivität, so empfiehlt zum Beispiel das deutsche "Bundesamt für Sicherheit in der Informationstechnik" den Einsatz von ReCoBS. (Bundesamt für Sicherheit in der Informationstechnik, 2006)

Jedoch können auch diese Verfahren nicht als komplett sichere Lösung für den Datenzugriff gewertet werden. Spätestens dann, wenn es um den Dateitransfer zwischen verschiedenen Umgebungen geht, zeigt sich, dass eine komplette Abtrennung aller Segmente beinahe ein unmögliches Unterfangen ist.

Im Falle von Sicherheitslücken im Hypervisor virtuellen Maschinen oder eines Kontrollservers von "Remote-Controlled Browsers Systems" kann der Einsatz solcher Lösungen sogar potentiell schädlich sein. Erst vor kurzem (im Febr. 2014) wurde in der Software "Jetro Cockpit Secure Browsing" eine Lücke gefunden mit der alle verbundenen Geräte vom Angreifer kontrolliert werden konnten.[8]

4.4 Application Whitelisting

Beim Application Whitelisting wird dem Betriebssystem vorgeschrieben, nur als vertrauenswürdig definierte Programme auszuführen. Dies wird durch die Nutzung von elektronischen Signaturen sichergestellt.

Wird in einem solchem Setup ein unvertrauenswürdiges Programm geladen, so wird die Ausführung vom Betriebssystem verhindert. Dieses System wird grundsätzlich auch von vielen modernen AppStores genutzt, z.B. der Apple AppStore oder der PlayStore von Google.

Diese Vorgehensweise ist sehr erfolgsversprechend, die Gefahr einer unabsichtlichen Ausführung von Schadsoftware wird damit stark minimiert. Problematisch ist allerdings die Qualitätssicherung. Irgendjemand muss definieren, welche Software gutartig ist. Und selbst bei gutartiger Software kann nicht definitiv sichergestellt werden, dass diese keine ausnutzbaren Sicherheitslücken enthält.

4.5 Virenscanner

Antiviren-Lösungen gelten heutzutage als durchaus umstritten, basiert die Erkennung zum grossen Teil doch auf signaturbasierter Erkennung (d.h. diese Software wird von vielen Personen eingesetzt und ist daher vermutlich gutartig) und nicht auf heuristischen Merkmalen (d.h. diese Software greift auf enorme Dateimengen in kurzer Zeit zu und sie ist daher vermutlich bösartig).

(Strobel, 2014) wagte sogar die Aussage, dass "[…] die Erkennungsrate klassischer Antivirenprodukte gerade bei gezielten Attacken enttäuscht", diese Behauptung wird auch vom bekannten amerikanischen Journalisten Brian Krebs untermauert. (Krebs, 2012)

Auch die Erfahrung von Compass belegt, dass Virenscanner keineswegs einen adäquaten Schutz gegen gezielte Angriffe bieten. Dank quelloffenen Frameworks wie dem Veil-Framework[9], welche den Inhalt der Dateien derart verschleiern, dass nur wenige Virenscanner diese als bösartig erkennen.

In einem Versuch hatte die UAB (University of Alabama) alle Emails, welche an ihre Studenten und Lehrkörper verschickt wurden, durch den Onlineservice VirusTotal[10] checken lassen. Dieser Service gehört mittlerweile zu Google und testet mit mehr als 42 Virenscannern, ob Dateien potentiell bösartig sind.

[8] Vgl. http://blog.quaji.com/2014/02/remote-code-execution-on-all-enterprise.html
[9] Vgl. https://www.veil-framework.com
[10] Vgl. https://www.virustotal.com/about/

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Datum	Absenderkennung	Bösartige Software	Initiale Erkennungsrate	Erkennungsrate nach 30 Tagen
20.06.2012	Verizon Wireless	BlackHole Exploit Kit > Generic Bad thing	3 von 42	4 von 42
20.06.2012	UPS + DHL	Zipped .EXE > Generic Bad Thing	4 von 42	6 von 42
19.06.2012	USPS	Zipped .EXE > SpyEye/Cridex/Bredolab	5 von 42	10 von 42

Tabelle 2 - Erkennungsrate von Antivirenscannern (Quelle: (Krebs, 2012)**)**

Die Ergebnisse dieses Versuchs sind durchaus eindrücklich, zeigt er doch auf, dass ein Grossteil der Viren erstmals – falls überhaupt – nur von wenigen Scannern erkannt wird und selbst 30 Tage nach der Initialerkennung viele Virenscanner die Malware immer noch nicht erkennen.

Genau dies zeigt auch die Problematik bei der Nutzung von Virenscannern auf: So sind zwar die Chancen hoch, dass ein normaler Angriff erkannt und blockiert wird. Doch gegen gezielte Angriffe stellen Virenscanner keineswegs einen sinnvollen und brauchbaren Schutz dar.

4.6 Erkennung von Verhalten und statistischen Anomalien

Die Erkennung von statistischen Anomalien und nicht normalem Datenverkehr ist Kernpunkt dieser Whitepapers. Sie stellt eine äusserst effektive Möglichkeit dar, um festzustellen, ob sich in einem Netzwerk Angreifer befinden.

Bei diesem Vorgehen wird vorgängig definiert, wie legitimer und illegitimer Datenverkehr aussieht. Basierend auf diesen Daten können dann Regeln und Heuristiken erstellt werden mit denen bösartiges Verhalten gefunden werden kann.

Dies ist grundsätzlich auch der Ansatz, welcher von modernen Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) genutzt wird. Aufgrund der enormen Vielfalt von Angriffen werden rein automatisierte Erkennungsversuche jedoch niemals in der Lage sein, alle Angriffe zu erkennen. Wenn dies jedoch mit einer manuellen Analyse verbunden wird, sind die Ergebnisse sehr aussagekräftig.

4.7 Reputationsdatenbanken

Reputationsdatenbanken stellen eine bewährte Methode da, um bösartigen oder gutartigen Traffic voneinander zu unterscheiden. In einer Reputationsdatenbank werden bösartige und gutartige Systeme aufgelistet. Es gibt grundsätzlich zwei verschiedene Arten von Reputationsdatenbanken:

- Bad Known Hosts
  - Zusammenstellung von als *bösartig* bekannten Domains und IP Adressen.
  - Es handelt sich oft um öffentliche Listen, welche Command and Control Server von Malware auflisten.
- Good Known Hosts
  - Zusammenstellung von als *gutartig* bekannten Domains und IP Adressen.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- Muss für jeden Fall einzeln erstellt werden, da nicht klar ist, welche Verbindungen als akzeptabel angesehen werden.

Ein Beispielsauszug aus der Reputationsdatenbank "malwaredomains.com" kann im nachfolgenden Codebeispiel gefunden werden. Eine aktuelle Auflistung aller gängigen Datenbanken kann in Tabelle Tabelle 3 auf Seite 21 gefunden werden.

```
##      if you do not accept these terms, then do not use this information.
##           notice notice duplication is not permitted
## nextvalidation   domain                    type         dateverified

   20161231         retro-7-3.cz.cc           harmful      20131227
   20160601         x0a.in                    iframe       20131226
   20160601         x0c.ru                    malware      20131226
   20160601         mixgrouptravel.cn         malware      20131226

[CUT BY COMPASS]
```

Die öffentlich erhältlichen Datenbanken sind jedoch immer ein zweischneidiges Schwert. Zwar können diese durchaus hilfreich beim auffinden von bösartigen Endpunkten sein, aber die Integrität, Vertrauenswürdigkeit sowie die Aktualität kann keinesfalls garantiert werden. Daher sollten diese in jedem Fall nur als Ergänzung eingesetzt werden und die Ergebnisse in jedem Fall hinterfragt werden. Es ist grundsätzlich davon abzuraten, öffentliche Datenbanken zur vollständigen Erkennung als "Good Known Hosts" einzusetzen.

Der Einsatz von massgeschneiderten individuellen Reputationsdatenbanken ist jedoch unumgänglich, da dadurch das Grundrauschen äusserst effektiv eingeschränkt werden kann. Details wie dies mittels Splunk umgesetzt werden kann, sind im Kapitel 6.4.2 auf Seite 47 zu finden.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Name	Betreiber	Inhalt	IP-Blocklist	Domain Blocklist
SpyEye Tracker	abuse.ch	SpyEye Kontroll server	spyeyetracker.abuse.ch/blocklist.php?download=ipblocklist	spyeyetracker.abuse.ch/blocklist.php?download=domainblocklist
Cyber Tracker	CyberTracker	Malware Kontroll server	-	cybercrime-tracker.net/all.php
malc0de	Malc0de	Hosts welche in den letzten 30 Tagen Malware verteilt haben.	malc0de.com/bl/IP_Blacklist.txt	malc0de.com/bl/BOOT
Palevo Tracker	abuse.ch	Palveo Kontroll server	palevotracker.abuse.ch/blocklists.php?download=ipblocklist	palevotracker.abuse.ch/blocklists.php?download=domainblocklist
Feodo Tracker	abuse.ch	Feodo Kontroll server	feodotracker.abuse.ch/blocklist/?download=ipblocklist	feodotracker.abuse.ch/blocklist/?download=domainblocklist
ZeuS Tracker	abuse.ch	ZeuS Kontroll server	zeustracker.abuse.ch/blocklist.php?download=badips	zeustracker.abuse.ch/blocklist.php?download=baddomains
Malware Domains	MalwareDomains	Zusammenstellung diverser Malware Server.	-	mirror2.malwaredomains.com/files/justdomains
bt_proxy	BlueTack	Zusammenstellung offener Proxys Server.	list.iblocklist.com/?list=bt_proxy&fileformat=p2p&archiveformat=gz	-
DROP	SpamHaus	Gekaperte IP Ranges	list.iblocklist.com/?list=sh_drop&fileformat=p2p&archiveformat=gz	-

Tabelle 3 - Existierende frei erhältliche Reputationsdatenbanken

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.8 Übersicht über die Vor- und Nachteile

In der folgenden Tabelle wird ein Überblick über die verschiedenen Erkennungsmechanismen sowie deren Vor- und Nachteile geboten.

Da Compass keine Empfehlungen für den Einsatz von Produkten abgibt, wurde keine Rücksicht auf spezifische Programme genommen.

Ansatz	Bereich	Beschreibung	Vorteile	Nachteile
Sanitisation: Entfernung von Code (#4.1)	DMZ-Struktur	Konvertierung aller übertragenenen Dateien in ein anderes Dateiformat.	✦ Erfolgswahrscheinlichkeit von Angriffen wird stark verringert.	✦ Dateiaustausch mit Externen wird deutlich erschwert. ✦ Lediglich präventive Wirkung, keine Erkennung von Angriffen. ✦ Zusätzlicher Kommunikations kanal mit vertrauenswürdig en Drittparteien ist notwendig.
Beobachtung des Codes bei Ausführung in virtuellen Maschinen (#4.2)	DMZ-Struktur	Ausführung von übertragenen Dateien in abgesicherten virtuellen Maschinen und verhaltensbasierende Analyse.	✦ Ist in der Lage triviale Malware zu erkennen.	✦ Benötigt geraume Zeit bis Dateien überprüft worden sind. ✦ Malware ist in der Lage, virtuelle Maschinen zu erkennen und sich dort anders zu verhalten. ✦ Kann Initialinfektionen oftmals nicht vermeiden.
Gekapselte Ausführung von Browser und Mail (#4.3)	Lokal	Programme werden in in dedizierten Umgebungen ausgeführt und können nicht aufeinander	✦ Sicherheitslücken betreffen jeweils nur ein einzelnes Programm und nicht das gesamte Betriebssystem.	✦ Dateiaustausch wird erschwert. ✦ Sicherheitslücken in den Serverkomponen

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Ansatz	Bereich	Beschreibung	Vorteile	Nachteile
		zugreifen.		ten kann zur Übernahme des gesamten Netzs führen.
Application Whitelisting (#4.4)	Lokal	Nur digital signierte Programme, welche von einem Administrator zugelassen wurden werden vom Betriebssystem ausgeführt.	✦ Die unabsichtliche Ausführung von Schadsoftware kann zuverlässig verhindert werden.	✦ Schützt nicht gegen Sicherheitslücken in den Programmen. ✦ Enorm aufwändig.
Virenscanner (#4.5)	Lokal	Analysiert, ob die Datei möglicherweise Schadsoftware enthält.	✦ Zuverlässiger Schutz gegen primitive Angriffe.	✦ Basiert oftmals nur auf signaturbasierten Checks und erkennt daher nur bekannte Viren. ✦ Lässt sich von erfahrenen Angreifern relativ einfach umgehen.
Erkennung von Verhalten und statistischen Anomalien (#4.6)	LAN / DMZ Struktur	Analyse, ob das festgestellte Verhalten in den Logdaten bösartigem Datenverkehr ähnelt.	✦ Auch geeignet zur nachgängigen Analyse. ✦ Durch eine manuelle Analyse kann prinzipbedingt viel mehr gefunden werden als durch automatisierte Prozesse.	✦ Enorm zeitaufwändig.
Reputations-datenbanken (#4.7)	-	Datenbank, welche festhält ob ein Host gut- oder bösartig ist.	✦ Geeignet, um festzustellen ob ein System mit einem bekannten Botnet kommuniziert. ✦ Kann auch als Kommunikationsmatrix sinnvoll sein.	✦

Tabelle 4 - Übersicht über die verschiedenen Ansatzpunkte

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Es lässt sich also festhalten, dass jeder dieser Ansätze durchaus Vor- und Nachteile besitzt und keine Methode ein Allheilmittel ist und eine umfassende Sicherheit gewährleisten kann.

In diesem Whitepaper wurde als thematischer Schwerpunkt primär die Erkennung von Verhalten und statistischen Anomalien mittels Splunk gewählt sowie die Benutzung von Reputationsdatenbanken. Die anderen Methodiken wurden lediglich vollständigkeitshalber erwähnt, um das Feld abzustecken.

4.9 Kommunikationskanäle von APT

Allein der Begriff des APT macht klar, dass es keine perfekte Methodologie zur Erkennung von APT gibt. Jedoch basieren APT im Endeffekt auch lediglich auf Malware, welche nur äusserst geklügelt aufgebaut ist, letztendlich aber zwangsweise immer noch auf die gleichen Kommunikationskanäle setzen muss. Auch wenn der angebliche Supervirus "BadBIOS" in der Lage sein soll, über Töne knapp unterhalb der Ultraschallgrenze zu kommunizieren. (Himmelein, 2013)

In den anschliessenden Kapiteln wird daher auf die wohl am häufigsten gewählten Kommunikationskanäle eines bösartigen Programmes eingegangen.

4.9.1 DNS Tunnel

DNS ist die Abkürzung für das globale "Domain Name System", vereinfacht lässt sich dies als eine Art Telefonbuch für Domainnamen beschreiben. Dieses Telefonbuch enthält die Zuordnungen von Domainname und IP-Adressen.

Vereinfacht zusammengefasst funktioniert dies in einem typischen Firmennetzwerk folgendermassen:

1. Ein Nutzer will die Seite "www.csnc.ch" aufrufen.
2. Der interne DNS Server der Unternehmung schaut nach, ob die Domain bereits im Cache ist, dies ist hier nicht der Fall.
3. Der interne DNS Server fragt bei einem der dreizehn zentralen Rootserver nach, welcher Registrar für die Top-Level-Domain ".ch" zuständig ist.
4. Der Rootserver gibt an, dass ein Server der SWITCH diese Zone verwaltet und sendet eine IP Adresse zurück.
5. Der interne DNS Server fragt beim SWITCH DNS Server nach, welche Domainserver für die Zone "csnc.ch" zuständig sind. Es wird die IP Adresse des DNS Servers von der Compass Security AG zurückgegeben.
6. Der interne DNS Server sendet eine Anfrage, welche IP "www.csnc.ch" besitzt an den DNS Server der Compass Security AG. Es wird die IP 212.254.246.115 zurückgegeben.

Das Domain Name System hat also eine äusserst wichtige Position inne und daher sind die DNS Anfragen oftmals nicht begrenzt. Ohne DNS wäre das heutige Internet nicht in einer sinnvollen Art und Weise nutzbar.

Dies ist jedoch auch die Gefahr dahinter, denn was hindert Malware daran, DNS Anfragen als Covert Channel zu benutzen? So können zum Beispiel Textdateien oder Befehle relativ simpel übertragen werden, muss die Malware doch nur Anfragen wie "InhaltEinerGeheimenDatei.evil.com" senden, welche an den bösartigen DNS Server übertragen werden. Eine vereinfachte Abbildung dieses versteckten Kommunikationskanales ist in Abbildung 8 ersichtlich.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

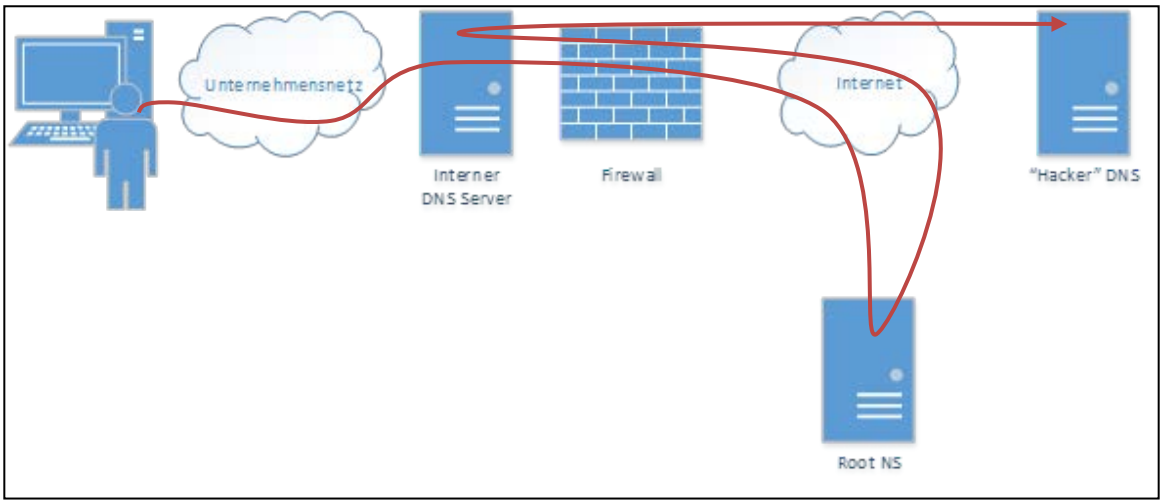


Abbildung 8 - DNS Tunnel

4.9.2 HTTP(S)

Das HTTP-Protokoll ist wohl eines der meistgenutzten Protokolle schlechthin. Bei jedem Aufruf einer Website geschieht dies über HTTP oder dessen verschlüsselten Pendant HTTPS.

Das World-Wide-Web ist wohl derzeit eine der mächtigsten Kommunikationskanäle, welche die Menschheit besitzt. Der Zugriff ist darum in vielen Fällen auch nicht eingeschränkt. Für einen Angreifer ist dies darum ein äusserst komfortabler Kommunikationskanal. Im Rahmen dieses Whitepapers wurde daher eine Heuristik zur Erkennung von ungewöhnlichem HTTP Verkehr entwickelt. Mehr darüber ist in Kapitel 6.4.1.1 zu erfahren.

4.9.3 Mail

Zwar benutzen nach Aufassung von Compass Security eher wenige bösartige Schadprogramme E-Mails als Kommunikationskanal. Aber für einen technisch weniger geschulten Mitarbeiter stellen E-Mails eine valable Möglichkeit zur Exfiltration von internen Daten da.

4.9.4 Chat

Dass Schadprogramme Chatprokolle wie IRC benutzen, um miteinander zu kommunizieren, ist keine Seltenheit[11].

Ein zuverlässiger Schutz gegen derartige Kommunikationskanäle ist es, in diesem Fall sicherzustellen, dass nur über zugelassene Protokolle wie HTTP zu externen Servern kommuniziert werden kann.

[11] Vgl. http://www.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

5 Big Data Analysis

5.1 Einführung

Big Data Analysis bezeichnet die Analyse von Datenmengen, welche dermassen gross und komplex sind, dass es mit den üblichen Tools beinahe unmöglich ist, diese zu analyiseren. Der Big Data-Experte Tom White stellt dabei eine interessante Behauptung auf, nämlich dass Big Data auch sehr klein sein kann und nicht alle grossen Datensätze zwangsweise "Big Data" sind. Für Tom White zählen so auch zum Beispiel schon grössere Fotoansammlungen als Big Data. (White, 2012)

Nach dieser Annahme gilt also grundsätzlich alles als Big Data, was nicht mit herkömmlichen Programmen in einem vernünftigen Zeitraum sinnvoll verwaltet werden kann. Für diese Kategorie von Daten braucht es also neuartige Programme und Vorgehensweisen.

Diese Aussage gilt umso mehr für die Analyse von Logdaten eines Netzwerkes. Zwar mag die rein physische Datenmenge sich nur auf einige Gigabyte zu beschränken, wenn man sich aber vor Augen hält, dass dies reine Textformate mit mehreren Millionen oder gar Milliarden Einträgen sind, zeigt sich, dass sich diese mit altbekannten Mitteln nicht mehr angemessen verwalten lassen.

Auch wenn es leider keine öffentlichen Statistiken dazu gibt, wie viele Systemadministratoren die Logs ihrer Systeme regelmässig begutachten, so zeigen Erfahrungswerte, dass dies in äusserst wenigen Betrieben regelmässig der Fall ist. Aufgrund der enormen Menge an Logdaten korreliert der Aufwand oftmals keineswegs mit den Ergebnissen.

5.2 Problemstellungen

In derartig grossen Datensätzen ist es nicht mehr möglich und sinnvoll den Datenverkehr von jedem einzelnen System zu analysieren, dort müssen komplett andere und neuartige Ansätze gewählt werden, um eine effiziente Analyse zu garantieren:

- Erkennung von Anomalien mittels Heuristiken
    - Um potentiell bösartige Verhaltensmuster zu erkennen ist es von Nöten, sich zu überlegen welche Verhaltensmuster als potentiell gutartig gelten und dafür Heuristiken zu implementieren. So sind zum Beispiel einzelne HTTP Anfragen ohne nachfolgendes Laden von eingebetteten Ressourcen ein Indiz für eine Malware, welche mit den Command and Control Server kommuniziert.
- Erkennung von legitimen Datenverkehr mittels Heuristiken
    - Ebenso wichtig ist es, in einem Datenset den definitiv gutartigen Datenverkehr herauszufiltern.
- Erkennung von "good-known" und "bad-known" Endpunkten
    - Nicht bei jedem Datenpaket ist es möglich, diese mittels einer heuristischen Analyse als gut- oder bösartig einzustufen. In solchen Fällen empfiehlt es sich dann ganze Datenströme zu analysieren. So können zum Beispiel Verbindungen zwischen einem internen NTP Server und dem internen Netzwerk als "good-known" eingestuft werden und so nach und nach alle uninteressanten Verbindungen ausgeschlossen werden.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6 Erkennung von APT mittels Splunk

Splunk eignet sich als Allrounder im Bereich der Big-Data Analyse für fast jeden Anwendungszweck. So monitoren unter anderem Verisign[12] oder UniCredit[13] die interne Netzwerkinfrastruktur mittels Splunk, während Unternehmen wie SWISSLOS[14] damit die Konversionsraten der Nutzer untersuchen.

Die mächtigen Suchfunktionen von Splunk erlauben einem Analysten beinahe unbeschränkte Möglichkeiten zur Analyse. In den nachfolgenden Kapiteln wird darauf eingegangen, wie Daten importiert und anschliessend analysiert werden können.

Die nachfolgenden Schritte setzen eine funktionierende Splunk Installation nach Herstellervorgabe voraus.[15]

6.1 Import von Daten

Der erste Schritt, um Daten analysieren zu können, ist der Import relevanter Daten. Dieser Prozess kann in wenigen Schritten erledigt werden.

1. Auswahl von *Add Data* auf dem Startscreen von Splunk

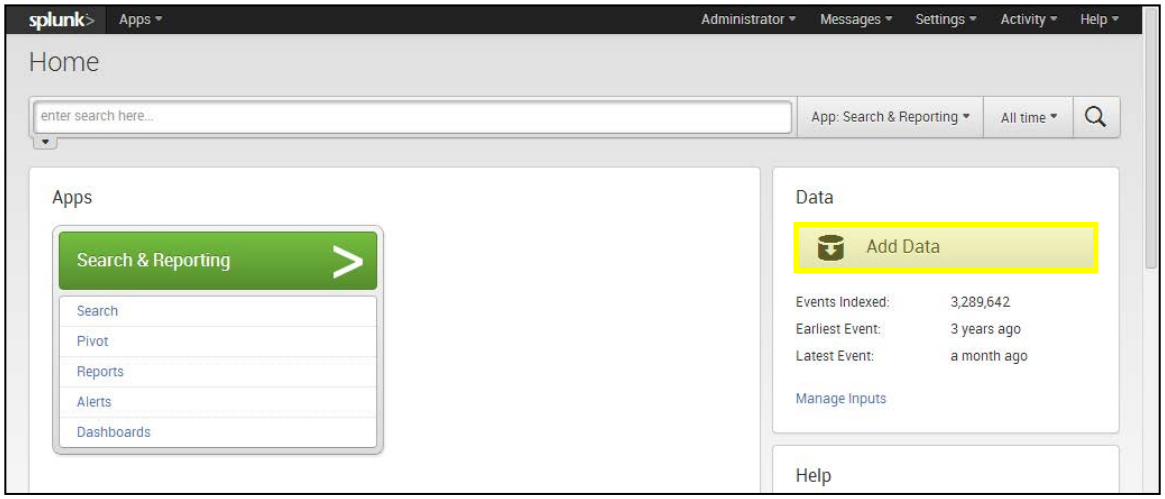


Abbildung 9 - Startseite von Splunk

[12] Vgl. http://www.splunk.com/view/splunk-at-verisign/SP-CAAAFNP
[13] Vgl. http://www.splunk.com/view/splunk-at-unicredit/SP-CAAAJC8
[14] Vgl. http://www.splunk.com/view/splunk-at-swisslos/SP-CAAAHSD
[15] Vgl. http://docs.splunk.com/Documentation/Splunk/6.0.2/Installation/InstallonLinux

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2. Als Datenquelle sollte *From files and directories* ausgewählt werden.

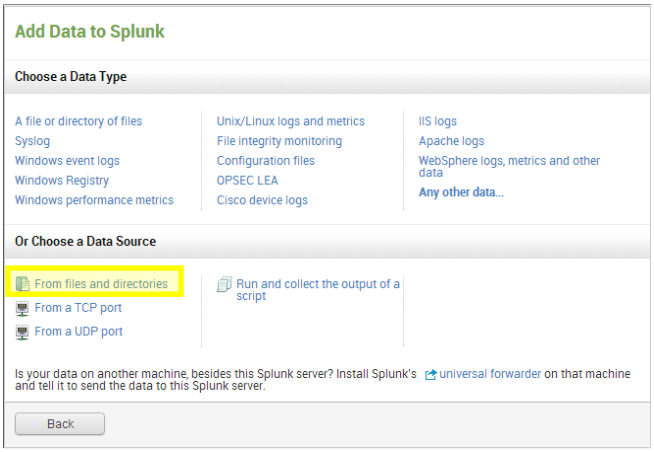


Abbildung 10 - Import von Daten mit Splunk

3. Die Vorschau sollte mit *Skip preview and manually configure your input* übersprungen werden.

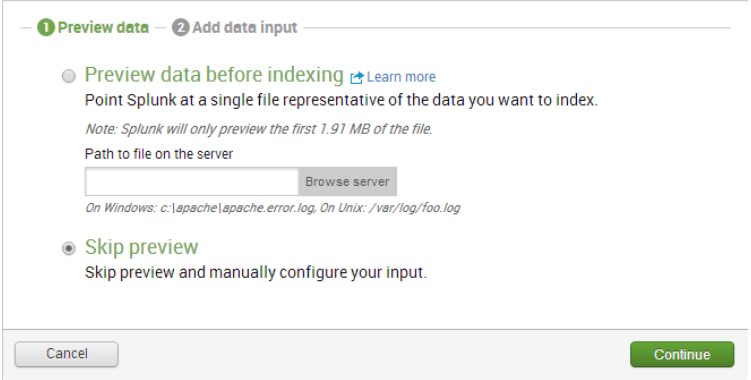


Abbildung 11 - Vorschau von Daten in Splunk

4. Nun bietet Splunk die folgenden drei Optionen an:

   a. *Continuously index data from a file or directory this Splunk instance can access*
      - Überwacht und indexiert den Inhalt einer Datei oder eines Ordners fortlaufend.
        ⇨ Dies ist die empfohlene Option für eine Analyse, dies erlaubt einem Analysten Logdateien bei Bedarf zu ergänzen.

   b. *Upload and index a file*
      - Indexiert eine hochgeladene Datei.

   c. *Index a file once from this Splunk server*
      - Indexiert eine lokale Datei, ohne auf zukünftige Änderungen Rücksicht zu nehmen.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

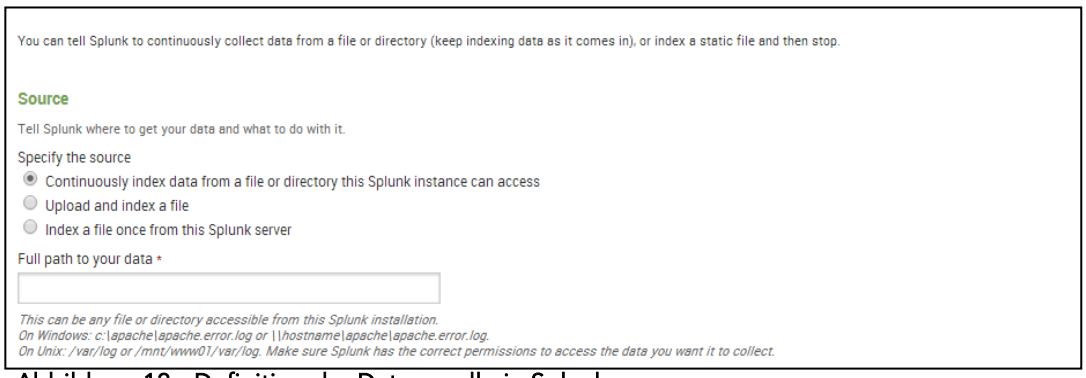


Abbildung 12 - Definition der Datenquelle in Splunk

5. Beim Import von Daten muss nun im Feld "*Set the source type*"der entsprechende Datentyp gewählt werden. Dieser kann in Kapitel 7 auf Seite 50 nachgeschlagen werden.

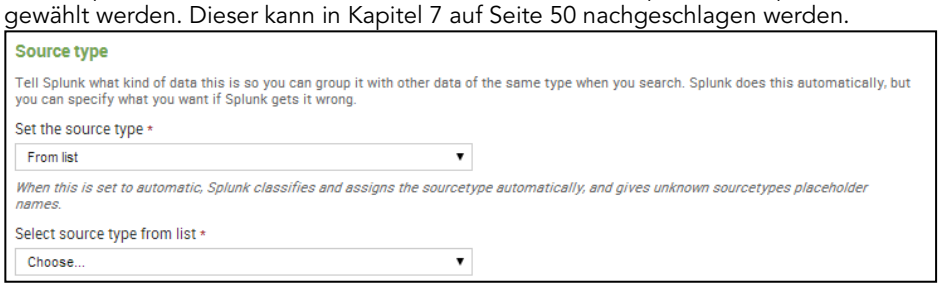


Abbildung 13 - Definition des Datentypes in Splunk

Detaillierte Schritt für Schrittanleitungen sind auf der Website des Herstellers zu finden: www.splunk.com

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.2 Suchbefehle

Splunk benutzt die SQL-ähnliche Search Processing Language (kurz: SPL). Die komplette Referenz der Suchbefehle kann der Herstellerseite entnommen werden.[16]

Eine Auswahl der während dieser Arbeit benutzen Suchbefehle ist in den nachfolgenden Abschnitten mit Beispielen jeweils dokumentiert.

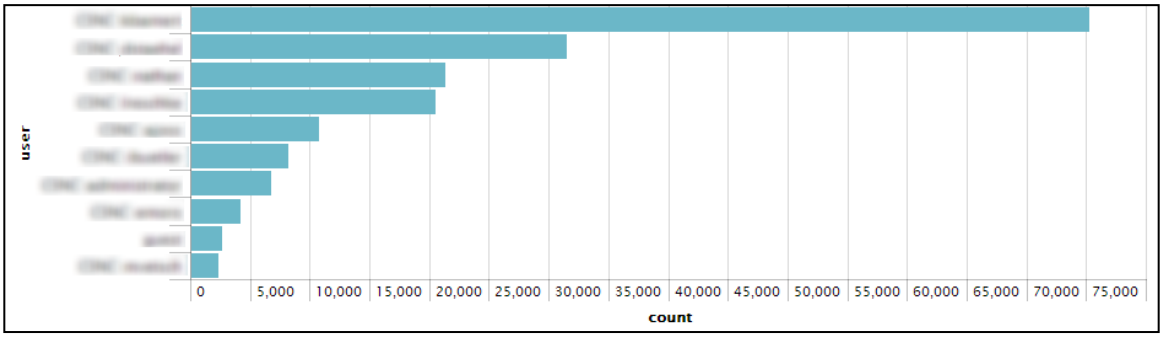
6.2.1 top

Zeigt die häufigsten Werte eines Feldes an. Dieser Befehl kann auch in Verbindung mit einer Visualisierung genutzt werden.

Beispiel: Zeige die Benutzer mit den 10 meisten Aktionen im Index "smb" an.

```
index=smb | top limit=10 user

user                count        percent
john.doe            75236        38.563184
alexa.muster        31490        16.140606
tatjana.mustermann  21280        10.907339
pia.betschard       20528        10.521892
kevin.meier         10738        5.503901
ingo.meckert        8120         4.162011
gabriela.martic     6684         3.425971
katja.simmler       4130         2.116885
thomasz.arukovic    2636         1.351116
salome.schmid       2312         1.185045
```



6.2.2 head

Zeige die ersten *n* Ergebnisse an.

Beispiel: Zeige die neusten 3 Logeinträge im Index "smb" an.

```
index=smb | head 3

2014/02/05 11:58:02,10.14.0.70,ameier,write,File,165
Bytes,/shares/admin/inventory/licenses/~$licenses_V1.0.xlsx
2014/02/05 11:58:02,10.14.0.70,ameier,create,File,0
Bytes,/shares/admin/inventory/licenses/~$licenses_V1.0.xlsx
```

[16] Vgl. http://docs.splunk.com/Documentation/Splunk/6.0.2/SearchReference/

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
2014/02/05 11:58:02,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
```

6.2.3 search

Suche nach Ereignissen, welche eine bestimmte Bedingung erfüllen.

Beispiel: Zeige Ereignisse, welche im Feld "action" den Wert "read" besitzen im Index "smb".

```
index=smb | search action="read"

2014/02/05 11:58:02,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:02,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
```

6.2.4 eval

Erstellt ein neues Feld für jedes Ereignis basierend auf einem Befehl.

Beispiel: Weise jedem Ereignis ein Feld "full_name" zu, welches sich aus dem Vor- und Nachnamen zusammensetzt.

```
index=smb | eval full_name=name+" "+firstname

2014/02/05 11:58:02,10.14.0.70,ameier,andreas meier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:02,10.14.0.70,ameier,andreas meier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,andreas meier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,andreas meier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,andreas meier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,andreas meier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
```

6.2.5 transaction

Fasse Ereignisse anhand eines ersten primären Ereignisses zusammen.

Beispiel: Fasse alle Ereignisse vom gleichen Benutzer im Index "smb" zusammen.

```
index=smb | transaction user

------------------------------ ameier ------------------------------
2014/02/05 11:58:02,10.14.0.70,ameier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:02,10.14.0.70,ameier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx 2014/02/05
11:58:01,10.14.0.70,ameier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
--------------------------------------------------------------------
```

6.2.6 replace

Ersetze Werte eines Feldes mit einem anderem Wert.

Beispiel: Ersetze alle Vorkommnisse von ameier mit "XXX" im Feld "user".

```
index=smb | replace ameier with XXX in user

2014/02/05 11:58:02,10.14.0.70,XXX,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:02,10.14.0.70,XXX,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,XXX,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
```

6.2.7 sort

Sortiere Suchergebnisse anhand eines spezifizierten Feldes.

Beispiel: Sortiere Ereignisse im Index "smb" nach aufsteigender Zeit.

```
index=smb | sort _time

2014/02/05 11:58:02,10.14.0.70,ameier,read,File,54.43 KB,
/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:02,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.70,ameier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
```

6.2.8 dedup

Entfernt Ereignisse, welche Felder mit identischen Werten beinhalten.

Beispiel: Entferne Ereignisse, welche den gleichen Wert im Feld file_name und user besitzen.

```
index=smb | dedup file_name user

2014/02/05 11:58:02,10.14.0.70,cfrey,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
2014/02/05 11:58:01,10.14.0.71,amaier,read,File,54.43
KB,/shares/admin/inventory/licenses/licenses_V1.0.xlsx
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.3 Common Pitfalls

Auch Splunk hat einige Tücken zu bieten, welche einem Neueinsteiger nicht direkt auffallen. Um den Einstieg zu vereinfachen, wird daher in dem anschliessenden Kapitel auf die Probleme beim Umgang mit Splunk eingegangen.

6.3.1 Gross-/Kleinschreibung

Splunk besitzt keine gängige Devise beim Umgang mit der Gross-/Kleinschreibung. Je nach Befehl wird diese anders interpretiert. In Tabelle 5 wird aufgelistet, welche Funktion wie reagiert.

	Sensitive	Insensitive	Beispiele
Befehle		X	TOP, top, sTaTs
Befehls Keywords		X	AS, BY, WITH, …
Suchbegriffe		X	Error, ERROR, Error
Statistische Funktionen		X	Avg, AVG, chart, …
Boolesche Funktionen	X		AND, OR, NOT
Feldnamen	X		host vs. HOST
Feldwerte		X	Host=localhost, host=LOCALHOST
Reguläre Ausdrücke	X		\d\d\d vs. \D\D\D
"replace" Befehl	X		error vs ERROR

Tabelle 5 - Case Sensitivity (Quelle: (Carasso, 2012))

6.3.1.1 anomalies

Splunk liefert das *anomalies* Kommando von Haus aus mit. Dieser Befehl sucht in einem Datenset nach sogenannten unerwarteten Ereignissen. Jedem Ereignis wird dabei ein *unexpectedness* Score zugewiesen, der aufgrund der Häufigkeit von ähnlichen Events in *P* vorherigen Ereignissen berechnet wird. Der Algorithmus ist dabei proprietär, wird aber mit folgender Formel ungefähr beschrieben:

$$unexpectedness = \frac{s(P\ and\ X) - s(P)}{s(P) + s(X)}$$

X entspricht dabei einem einzelnen Event, während *P* eine Ansammlung von vorherigen Events ist. *s()* ist hierbei eine Metrik wie ähnlich oder gleichmässig die Ereignisse verteilt sind. (Splunk Inc.)

Auch wenn dieser Befehl zwar verlockend klingen mag und durchaus auch bei der Analyse seine Existenzberechtigung hat, kann von der Verwendung dieses Befehls deutlich abgeraten werden. Bei Begutachtung der Definition des Kommandos wird klar, dass sich hiermit nur neu entstehende Bedrohungen einigermassen sinnvoll feststellen lassen. Durch das automatische Erlernen von Mustern werden auch potentiell schädliche Muster als legitim erachtet.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

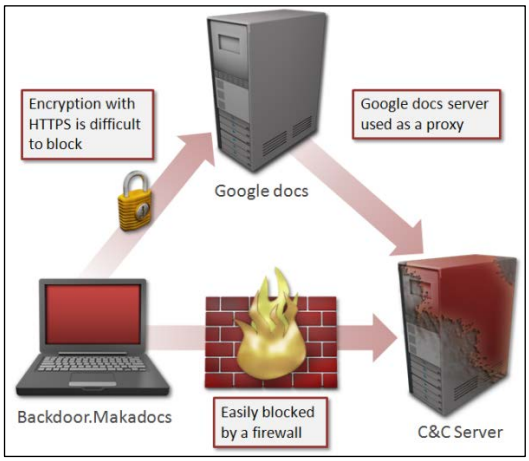


Abbildung 14 - Google Docs als Proxy

Der Befehl eignet sich daher eher für eine andauernde Analyse der Daten und nicht für eine Betrachtung im Nachhinein, da eine andauernde Bedrohung damit dann nicht mehr erkannt werden kann.

Daher ist es immer noch am besten, selbst gewisse simple Heuristiken zu erarbeiten, welche auf ungewöhnliches Verhalten hinweisen. Dies muss aber für jedes Protokoll einzeln erfolgen und ist darum äusserst aufwändig.

6.4 Empfohlene Suchabfragen

Auch wenn aufgrund der Natur eines APT davon ausgegangen werden kann, dass es nicht möglich ist, wirklich alle möglichen Angriffsmöglichkeiten zu entdecken, ist es dennoch sinnvoll, eine Art Standardvorgehen zu entwickeln, welches im Falle eines allfälligen Angriffes genutzt werden kann.

Im Folgenden wird daher auf die Erkennungsmethoden mittels Splunk eingegangen sowie Empfehlungen für Suchabfragen abgegeben:

- Heuristische Erkennung von Anomalien in einem Datenset (#6.4.1)
- Filterung von Bad Known / Good Known Hosts in einem Datenset (#6.4.2)

6.4.1 Feststellung von Anomalien

Eine der mächtigsten Funktionen von Splunk ist sicherlich die Erkennung von Anomalien in grösseren Datensets. Eine Anomalie definiert sich hierbei als unerwartetes Verhalten. Aufgrund der enormen Komplexität der verschiedenen Protokolle und deren verschiedenen Nutzungszwecken ist es jedoch unabdingbar, die Heuristiken zur Erkennung von unerwartetem Verhalten selbst zu definieren.

6.4.1.1 HTTP(S) Anomalien

Anomalien in ungeschützten HTTP oder HTTPS Verbindungen waren ursprünglich verhältnismässig einfach aufzuspüren. Doch moderne Webtechnologien wie WebSockets, AJAX und der massive Einsatz von Javascript haben die Messlate heutzutage deutlich höher angesetzt.

Erst kürzlich analysierte das amerikanische IT-Sicherheitsunternehmen Symantec gar eine Malware, welche Google Docs, ein Onlinebearbeitungsprogramm für Dokumente, als Proxy zur Kommunikation mit den Command and Control Servern nutzten. (Katsuki, 2012)

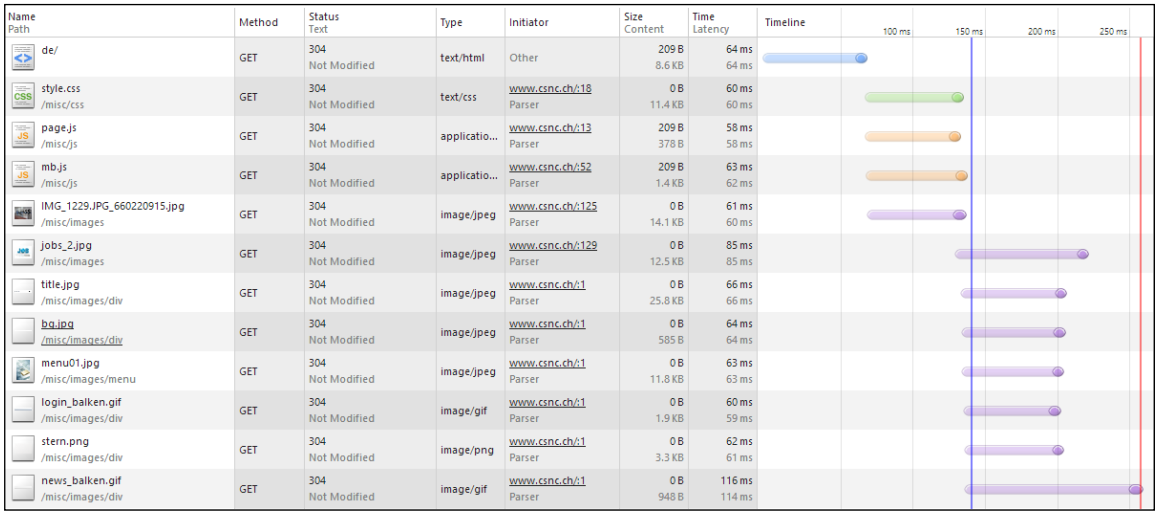
Dies macht klar, dass die Methoden zur Verschleierung eines Angriffes immer kreativer werden und so selbst mutmasslich vertrauenswürdige Verbindungen als potentiell kritisch angesehen werden müssen. Daher müssen neue Ansätze gewählt werden.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.4.1.1.1 Traffic

Bei Betrachtung eines typischen HTTP Requests zu einer Website mittels eines Webbrowsers wird klar, dass diese Requests oft weitere nach sich ziehen (vgl. Abbildung 15 - HTTP Request an www.csnc.ch). Dies sind zum Beispiel eingebettete Bilder, Skripte oder auch Stylesheets.

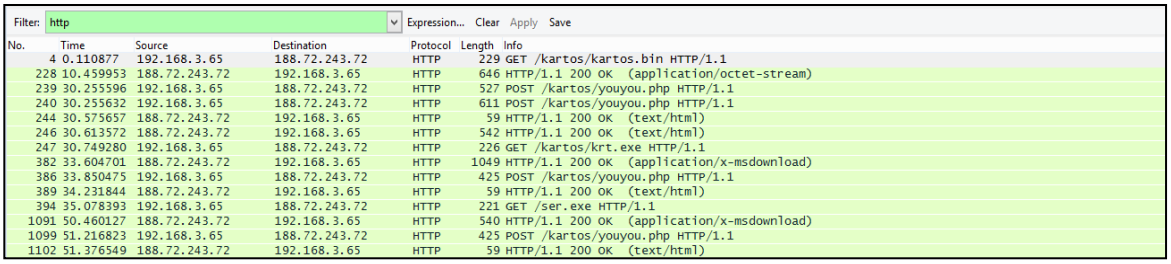


Name / Path	Method	Status / Text	Type	Initiator	Size / Content	Time / Latency	Timeline
de/	GET	304 Not Modified	text/html	Other	209 B 8.6 KB	64 ms 64 ms	
style.css /misc/css	GET	304 Not Modified	text/css	www.csnc.ch/:18 Parser	0 B 11.4 KB	60 ms 60 ms	
page.js /misc/js	GET	304 Not Modified	applicatio...	www.csnc.ch/:13 Parser	209 B 378 B	58 ms 58 ms	
mb.js /misc/js	GET	304 Not Modified	applicatio...	www.csnc.ch/:52 Parser	209 B 1.4 KB	63 ms 62 ms	
IMG_1229.JPG_660220915.jpg /misc/images	GET	304 Not Modified	image/jpeg	www.csnc.ch/:125 Parser	0 B 14.1 KB	61 ms 60 ms	
jobs_2.jpg /misc/images	GET	304 Not Modified	image/jpeg	www.csnc.ch/:129 Parser	0 B 12.5 KB	85 ms 85 ms	
title.jpg /misc/images/div	GET	304 Not Modified	image/jpeg	www.csnc.ch/:1 Parser	0 B 25.8 KB	66 ms 66 ms	
bg.jpg /misc/images/div	GET	304 Not Modified	image/jpeg	www.csnc.ch/:1 Parser	0 B 585 B	64 ms 64 ms	
menu01.jpg /misc/images/menu	GET	304 Not Modified	image/jpeg	www.csnc.ch/:1 Parser	0 B 11.8 KB	63 ms 63 ms	
login_balken.gif /misc/images/div	GET	304 Not Modified	image/gif	www.csnc.ch/:1 Parser	0 B 1.9 KB	60 ms 59 ms	
stern.png /misc/images/div	GET	304 Not Modified	image/png	www.csnc.ch/:1 Parser	0 B 3.3 KB	62 ms 61 ms	
news_balken.gif /misc/images/div	GET	304 Not Modified	image/gif	www.csnc.ch/:1 Parser	0 B 948 B	116 ms 114 ms	

Abbildung 15 - HTTP Request an www.csnc.ch

Malware folgt dieser Logik in den seltensten Fällen, typischerweise werden oft lediglich einzelne Anfragen an den Controlserver gesendet. Ein Beispiel dafür ist das bekannte trojanische Pferd "ZeuS". Die Sicherheitsfirma SourceFire stellt Beispiele der Initialkommunikation von ZeuS online jedermann im PCAP Format zur Verfügung. [17]

Wie in Abbildung 16 dargestellt, sendet der verseuchte Client gerade nur sieben Anfragen an den Server und es wird keinerlei Nebenrauschen durch das Laden von Daten wie Bildern oder Stylesheets verursacht.



Filter: http — Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4	0.110877	192.168.3.65	188.72.243.72	HTTP	229	GET /kartos/kartos.bin HTTP/1.1
228	10.459953	188.72.243.72	192.168.3.65	HTTP	646	HTTP/1.1 200 OK (application/octet-stream)
239	30.255596	192.168.3.65	188.72.243.72	HTTP	527	POST /kartos/youyou.php HTTP/1.1
240	30.255632	192.168.3.65	188.72.243.72	HTTP	611	POST /kartos/youyou.php HTTP/1.1
244	30.575657	188.72.243.72	192.168.3.65	HTTP	59	HTTP/1.1 200 OK (text/html)
246	30.613572	188.72.243.72	192.168.3.65	HTTP	542	HTTP/1.1 200 OK (text/html)
247	30.749280	192.168.3.65	188.72.243.72	HTTP	226	GET /kartos/krt.exe HTTP/1.1
382	33.604701	188.72.243.72	192.168.3.65	HTTP	1049	HTTP/1.1 200 OK (application/x-msdownload)
386	33.850475	192.168.3.65	188.72.243.72	HTTP	425	POST /kartos/youyou.php HTTP/1.1
389	34.231844	188.72.243.72	192.168.3.65	HTTP	59	HTTP/1.1 200 OK (text/html)
394	35.078393	192.168.3.65	188.72.243.72	HTTP	221	GET /ser.exe HTTP/1.1
1091	50.460127	188.72.243.72	192.168.3.65	HTTP	540	HTTP/1.1 200 OK (application/x-msdownload)
1099	51.216823	192.168.3.65	188.72.243.72	HTTP	425	POST /kartos/youyou.php HTTP/1.1
1102	51.376549	188.72.243.72	192.168.3.65	HTTP	59	HTTP/1.1 200 OK (text/html)

Abbildung 16 - Traffic eines ZeuS verseuchten Computers zum Command and Control Server

Die Abbildung von derartigen Mustern wäre für einen Malware Autor zwar keine grosse Kunst, dennoch wird dies häufig vernachlässigt. Eine Abfrage zur Erkennung dieser Muster sieht zum Beispiel so aus:

index="proxy_log" type!=CONNECT	Suche im Index "proxy_log" nach Ereignissen,

[17] https://labs.snort.org/papers/samples/zeus-sample-3.pcap

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

	welche nicht den Typ "CONNECT" besitzen.
sort 0 dst_domain,src_ip,_time	Ereignisse nach Domain, dann nach IP und dann nach Zeit sortieren, um diese gruppieren zu können.
transaction dst_domain src_ip maxspan=5m maxevents=-1	Gruppierung von allen Ereignissen von der gleichen Domain und IP in einem Zeitrahmen von fünf Minuten.
search type!=image/* AND type!=text/css AND type!=application/x-shockwave-flash AND type!=*/javascript AND type!=application/x-javascript AND type!=video/*	Ausschluss der Gruppen, welche den genannten Datentypen entsprechen. Dies sind Ressourcen, welche oft beim Besuch einer normalen Website nachgeladen werden.

Natürlich ist diese Art der Erkennung nicht perfekt und wird auch vielen gutartigen Datenverkehr als potentiell bösartig markieren. Dies sind unter anderem:

- Extern eingebundene Werbetracker, welche keine weiteren Nachfragen nach sich ziehen.
- APIs, welche von clientseitig installierten Programmen aufgerufen werden.
- Content Delivery Networks.
- Websiten, welche Technologien wie mod_pagespeed einsetzen, verursachen unter Umständen nur einen einzigen Request.

Im Rahmen einer Analyse kann ein *inputlookup* genutzt werden, um harmlose Domains auszuschliessen. Der volle Befehl sieht dann folgendermassen aus:

```
index="proxy_log" type!=CONNECT | sort 0 dst_domain,src_ip,_time | transaction
dst_domain src_ip maxspan=5m maxevents=-1 | search type!=image/* AND
type!=text/css AND type!=application/x-shockwave-flash AND type!=*/javascript AND
type!=application/x-javascript AND type!=video/* NOT [inputlookup safe_domains ]
```

safe_domains definiert dabei einen Lookup mit folgendem Schema:

```
dst_domain
*.dropbox.com
*.gravatar.com
*.google-analytics.com
safebrowsing.clients.google.com
```

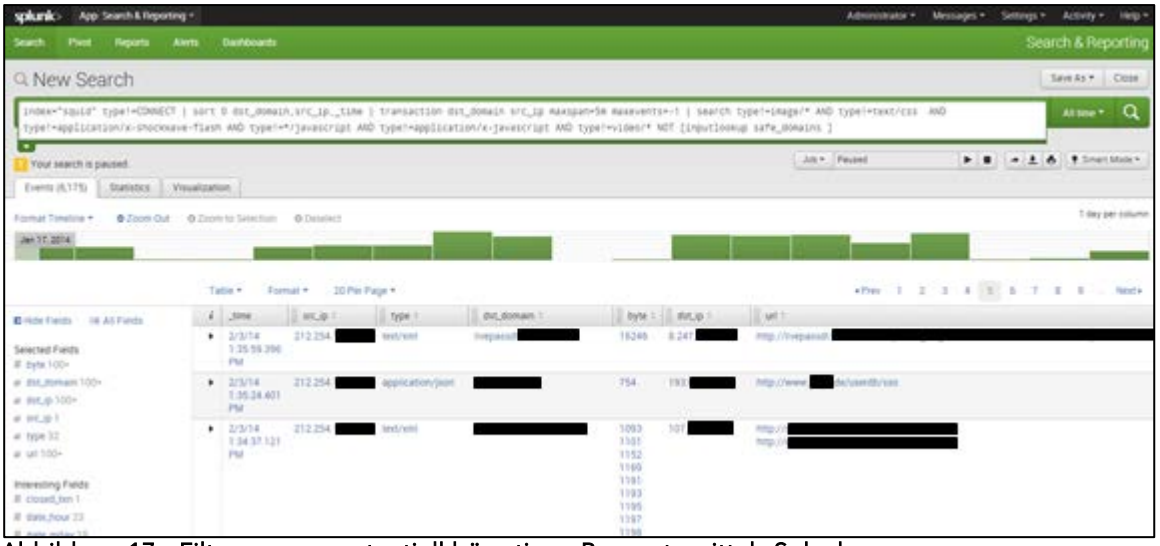


Abbildung 17 - Filterung von potentiell bösartigen Requests mittels Splunk

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

In Abbildung 17 sind die zeitlich gruppierten Abfragen zu sehen. Um einen noch schnelleren Überblick zu gewinnen, können auch alle Abfragen zu einer Domain ohne zeitliche Begrenzung gruppiert werden.

```
index="squid" type!=CONNECT | sort 0 dst_domain,src_ip,_time | transaction
dst_domain src_ip maxspan=5m maxevents=-1 | search type!=image/* AND
type!=text/css AND type!=application/x-shockwave-flash AND type!=*/javascript AND
type!=application/x-javascript AND type!=video/* NOT [inputlookup safe_domains ]
| transaction dst_domain src_ip maxevents=-1 | sort 0 dst_domain,_time
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.4.1.1.2 Referer

Gemäss RFC 2616 sollen HTTP Anfragen einen "Referer" *[sic!]* beinhalten, sofern die Anfrage eine andere Website als Ursprung hat und nicht direkt vom Nutzer eingegeben wurde. (Editor)

Ein Beispiel kann im nachfolgenden Request gesehen werden. Hier hat der Benutzer zuerst die Seite "/en/index.html" aufgerufen und besucht nun die Seite "/en/contact/". Rot hervorgehoben ist der Referer Header.

```
GET http://www.csnc.ch/en/contact/ HTTP/1.1
Host: www.csnc.ch
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:27.0) Gecko/20100101
Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csnc.ch/en/index.html
Connection: keep-alive
```

Malware nutzt diesen Header eigentlich nie (vgl. (Lewis, 2013)), er eignet sich daher recht zuverlässig als Filter zur Erkennung von potentiell bösartiger Software.

Rein konzeptionell wird diese Abfrage aber immer noch eine Vielzahl von gutartigen Anfragen als potentiell bösartig einstufen, unter anderem wären dies:

- API Anfragen von lokal installierten Applikationen
  - Viele Applikationen wie zum Beispiel Dropbox nutzen das HTTP Protokoll, setzen aber keinen Referer. Dies sollte in einer homogenen IT Infrastruktur aber kein Problem darstellen, da bekannt sein sollte, welche Hosts legitim sind und welche nicht.
- Aufruf der Startseite
  - Beim Aufruf der Startseite ist kein Referer gesetzt, jedoch verursacht diese weitere Requests mit einem Referer, daher kann dieser Request mittels einer Gruppierung als legitim erkannt werden.
- Direkter Aufruf einer Seite
  - Beim direkten Aufruf einer Seite wird ebenfalls kein Referer gesetzt, jedoch werden auch hier weitere Requests mit Referer abgesetzt und daher können auch diese Anfragen gefiltert werden.

Eine Abfrage dieser Requests würde wie folgt aussehen (der Suchparameter "referer" muss je nach eingesetzter Proxysoftware unter Umständen angepasst werden):

index="proxy_log"	Suche im Index "proxy_log"
sort 0 dst_domain,src_ip,_time	Ereignisse nach Domain, dann nach IP und dann nach Zeit sortieren, um diese gruppieren zu können.
transaction dst_domain src_ip maxspan=15m maxevents=-1	Gruppierung von allen Ereignissen von der gleichen Domain und IP in einem Zeitrahmen von fünfzehn Minuten.
search referer="-"	Suche nach Events ohne Referer.
eval hasReferer=mvfilter(match(referer, "http(s)*"))	In Transaktionen nach Events mit Referer suchen und diesem ein hasReferer Feld hinzufügen.
search NOT hasReferer=*	Nur Ereignisse ohne Referer anzeigen.

Die gesamte Abfrage sieht dann folgendermassen aus:

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
index="proxy_log" | sort 0 dst_domain,src_ip,_time | transaction dst_domain
src_ip maxspan=15m maxevents=-1 | search referer="-" | eval
hasReferer=mvfilter(match(referer, "http(s)*")) | search NOT hasReferer=*
```

6.4.1.1.3 User Agent

Der aufmerksamen Leser wird bei der Lektüre des vorherigen Codebeispiels festgestellt haben, dass es einen weiteren äusserst nützlichen Header gibt. Den sogenannten "User-Agent" Header. Die Nutzung dieses Headers wird als strikte Empfehlung vorgegeben.[18]

```
GET http://www.csnc.ch/en/contact/ HTTP/1.1
Host: www.csnc.ch
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:27.0) Gecko/20100101
Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csnc.ch/en/index.html
Connection: keep-alive
```

Jedoch ist es auch durchaus üblich, für Malware diesen Header zu besitzen, oftmals wird zur lokalen Firewallumgehung Code mittels DLL Injection in Browser injiziert. Anfragen, die dann über den Browser abgesetzt werden, besitzen auch dessen User Agenten.

Nichtsdestotrotz sollte diese Möglichkeit zur Analyse nicht vernachlässigt werden, so gibt es unter anderem mehrere verschiedene Indikatoren für eine Infektion:

Erkennung von Anfragen ohne User-Agent
Besonders Anfragen ohne User-Agent sollten unter die Lupe genommen werden. Derartige Anfragen sollten eigentlich nicht vorkommen.

index="proxy_log"	Suche im Index "proxy_log"
search NOT user_agent=*	Suche nach allen Ereignissen, welche im Feld "user_agent" einen leeren Wert stehen haben.

Die gesamte Abfrage sieht dann folgendermassen aus:

```
index="proxy_logs" | search NOT user_agent=*
```

Erkennung von unüblichen User-Agents
Mittels des nachfolgenden Befehls lassen sich User-Agents finden, welche nur geringe Requests bei einer zugeordneten IP besitzen. Da oftmals Malware nur sporadisch in Kontakt mit den Control-and-Command Servern steht, lassen sich so Anfragen erkennen, welche potentiell schädlich sind.

index="proxy_log"	Suche im Index "proxy_log"
rare user_agent by src_ip	Gruppiere alle Ereignisse anhand der IP-Adresse, zeige dann User-Agents einer IP Adresse, welche am wenigsten benutzt wurden.

```
index="proxy_logs" | rare user_agent by src_ip
```

[18] User agents SHOULD include this field with requests. (RFC 2616)

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Hosts mit mehreren User-Agents
Es ist für einen normalen Arbeitsplatz unüblich, mittels verschiedenen User-Agents zu kommunizieren. Mit dem folgenden Befehl lässt sich eine Auflistung der verwendeten User-Agents eines Endgerätes aufstellen.

index="proxy_log"	Suche im Index "proxy_log"
dedup src_ip user_agent	Entferne alle Einträge, welche die gleiche IP und den gleichen User-Agent besitzen
contingency src_ip user_agent usetotal=false	Erstelle eine Liste der benutzten User Agents pro IP.

```
index="proxy_log" | dedup src_ip user_agent | contingency src_ip user_agent
usetotal=false
```

Entwicklung der User-Agents über einen Zeitrahmen
Falls eine Malware zur Täuschung einen User-Agent mitsendet, so kann eine zeitliche Analyse mittels eines Timecharts Aufschluss darüber geben, ob ein User-Agent legitim ist. Besonders aussagekräftig ist dies jedoch nur, wenn die gesamte Unternehmung auf dem gleichen Patchstand ist.

index="proxy_log"	Suche im Index "proxy_log"
dedup src_ip user_agent	Entferne alle Einträge welche die gleiche IP und den gleichen User-Agent besitzen
timechart count by user_agent	Erstelle einen Zeitstrahl und zeige die Verbreitung der User-Agenten über diesen Zeitraum.

```
index="proxy_log"| dedup src_ip user_agent | timechart count by user_agent
```

6.4.1.2 DNS

Wie in Kapitel 4.9.1 bereits beschrieben, werden Daten oftmals mittels eines DNS Tunnels exfiltriert. Da DNS nicht als eigentlicher Kommunikationskanal entwickelt wurde, wird dieser Vektor oft stark vernachlässigt.

Nichtdestrotrotz sind DNS Tunnel oft äusserst leicht aufzuspüren, vorausgesetzt es werden die richtigen Daten geloggt, Ansätze hierfür sind unter anderem:

- Volumen des DNS Verkehrs pro IP Adresse
    - DNS Einträge besitzen alle eine sogenannte Time-to-Live (TTL); dieser Wert zeigt an wie lange eine Anfrage zwischengespeichert werden soll. Diese Werte reichen von wenigen Minuten (in Fällen von Failover Systemen) und mehreren Stunden (früher ein quasi-standard). Normalerweise sollten daher nicht allzuviele DNS Anfragen von einem einzelnen Host aus kommen.
- Anzahl von Subdomains einer Second-Level-Domain
    - Die meisten Domains besitzen nur wenige Subdomains, sollten Anfragen an eine Domain mit dutzenden Subdomains vorhanden sein, kann dies als Indikator für DNS Tunneling dienen.
- Länge einer Subdomain
    - Subdomains besitzen oft einen prägnanten Namen und sind daher kurzgehalten. So sind Subdomains wie "mail.example.com" häufiger anzutreffen als solche wie " fa54faekyy45crwme544dw43y68smqlc2jbv8ufq5qf5u4ehfbaq32bxxijb.example.com". Solche langen Namen enthalten oft versteckte Informationen.
- Regelmässige Anfragen für Domainnamen, welche nicht in den Alexa Topcharts stehen

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- Alexa stellt eine Liste der 1'000'000 meistbesuchten Websiten bereit. Bei Domains mit einer solchen Bekanntheit ist es unwahrscheinlich, dass sich ein DNS Tunnel darauf befindet.

Anzahl der DNS Anfragen pro IP Adresse

Unregelmässigkeiten bei der Anzahl der DNS Anfragen lassen sich am einfachsten mittels eines Zeitstrahls darstellen. Um die Anzahl der DNS Anfragen, welche von einer einzigen IP kommen, darzustellen, kann der folgende Befehl genutzt werden:

```
index="dns_log" | timechart count by src_ip limit=50 useother=false
```

Das Ergebnis einer solchen Abfrage ist in Abbildung 18 visualisiert, klar zu sehen ist, dass die meisten Systeme nur relativ wenige Anfragen machen, während einige wenige verhältnismässig viele Anfragen senden. Diese Systeme nutzen möglicherweise einen DNS Tunnel und die Anfragen der Hosts sollten einzeln analysiert werden.

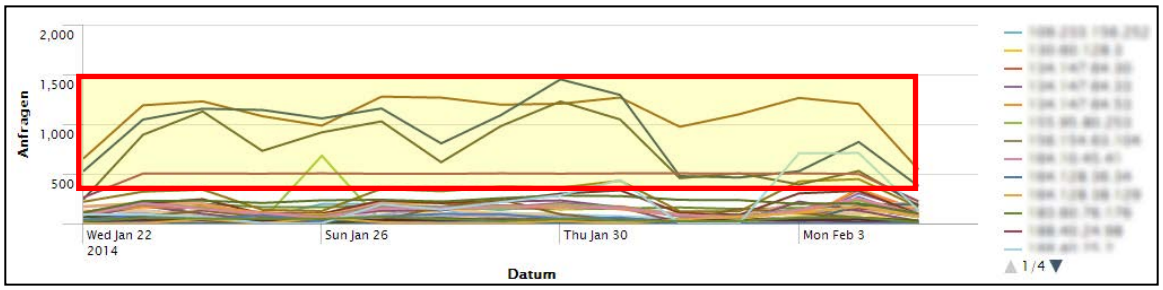


Abbildung 18 - DNS Anfragen pro IP Adresse mittels eines Zeitstrahls visualisiert

Anzahl von Subdomains einer Domain

Aufgrund der Kosten einer Domain kann die Annahme aufgestellt werden, dass für einen DNS Tunnel jeweils immer nur einzelne oder wenige Domainnamen genutzt werden.

Subdomains werden oft genutzt, um verschiedene Services unter einer Domain zu betreiben und den Nutzern zu erlauben, diese relativ einfach zu unterscheiden (z.B. mail.example.com und chat.example.com).
Daher ist die Anzahl der Subdomains oft in einem sehr überschaubaren Bereich und eine grosse Anzahl von Subdomains kann auf einen DNS Tunnel hindeuten.

```
index="dns_log" | eval domainname=lower(dst_sld) | eval
subdomain=lower(dst_subdomain) | dedup subdomain domainname | chart
count(subdomain) by domainname
```

Diese Abfrage ergibt dann als Ergebnis eine tabellarische Auflistung der Domains mit den meisten Subdomains. Dies sieht dann etwa so aus:

domainname	count(subdomain)
39asy.ru	19530
facebook.com	192
msn.com	123
heise.de	30

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

domainname	count(subdomain)
admin.ch	23
swisscom.com	16
educanet2.ch	13
sbb.ch	11
golem.de	10
csnc.ch	8

Länge von Subdomains

Um Daten zu transferieren, benutzen DNS Tunnel lange und kryptisch klingende Subdomains. Diese sind relativ einfach zu erkennen, weil es sehr unüblich ist, Subdomain so lang zu bennenen. Der Zweck einer Subdomain ist ja oftmals, die Erreichbarkeit eines Services zu vereinfachen.

```
index="dns_log" | eval subdomain=lower(dst_subdomain) | eval n=len(subdomain) |
dedup subdomain n | sort -num(n) | fields subdomain n
```

Das Ergebnis der obigen Abfrage ist dann eine Tabelle im folgenden Format:

Subdomain	n
bihihblol0ffgpekfhggdgemfjdcgnhghcdigmgnfkglhaffgbgiekggdidggga[...].dtt.[...]	97
bjcmfkhni0dgelgeddhcgndddcgmddfeekehecdehbgheffggogieeffdieab[...].dtt.[...]	97
bgghhjjmg0edebdhfigidhgbgjheehefglfgfjglejhkeoghfjfbgkeefcedebash[...].dtt.[...]	97
_ldap._tcp.9873ei3n-b05d-41d6-b781-dae189451705.domains._msdcs	62
abts-north-dynamic-234.254.165.128.airtelbroadband.in	53

Regelmässige Anfragen von Domains, welche nicht in den Alexa Top 1'000'000 stehen

Alexa Internet Inc. ist eine kalifornische Tochterunternehmung von Amazon, welche mittels der Alexa Toolbar Browsingverhalten trackt und an die firmeneigenen Server übermittelt. Dadurch ist Alexa in der Lage einigermassen realistische Schätzungen bezüglich der Beliebheit einer Website zu unternehmen.[19]

Diese Daten werden von Alexa kostenlos im Internet zur Verfügung gestellt, so lässt sich zum Beispiel via http://www.alexa.com/siteinfo/wikipedia.org die Popularität der Domain wikipedia.org feststellen, welche als sechst meistbesuchte Website dargestellt wird.

[19] http://www.alexa.com/company

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Zwar sind diese Daten weit von einer absolut zuverlässigen und fehlerfreien Datenquelle entfernt, aber um zu erfahren, ob eine Domain regelmässig legitim genutzt wird, ist es es ein guter Indikator.

Mittels der nachfolgenden Suchanfrage lassen sich alle aufgerufenen Domains im Format *subleveldomain.topleveldomain* auflisten:

```
index=dns_logs | eval dst_sld_tld=(lower(dst_sld+"."+dst_tld)) | dedup
dst_sld_tld | fields dst_sld_tld
```

Um Domains herauszufiltern, welche nicht in den Top 50000 der meistbesuchten Domain sind, kann der folgende Befehl genutzt werden:

```
index=dns_logs | eval dst_sld_tld=(lower(dst_sld+"."+dst_tld)) | dedup
dst_sld_tld | search NOT [inputlookup start=0 max=50000 alexa.csv ] | fields
dst_sld_tld
```

DNS Lookup Distribution World Map

Selbst trotz der Globalisierung ist es äusserst unüblich, dass Netzwerkverbindungen in jedes Land der Welt auftreten. So wird ein Mitarbeiter einer Schweizer Grossunternehmung zum Beispiel selten legitimen Datenverkehr mit Ländern wie Nordkorea oder Pakistan haben.

Die Google Maps Erweiterung für Splunk[20] bietet die Möglichkeit, die Herkunft von IP Adressen geografisch auf einer Weltkarte darzustellen. Dafür kann der folgende Befehl genutzt werden:

```
index=dns_logs | geoip dst_ip
```

Das Ergebnis ist dann eine interaktive Weltkarte, bei welcher die Herkunft der IP Adressen hervorgehoben wird.

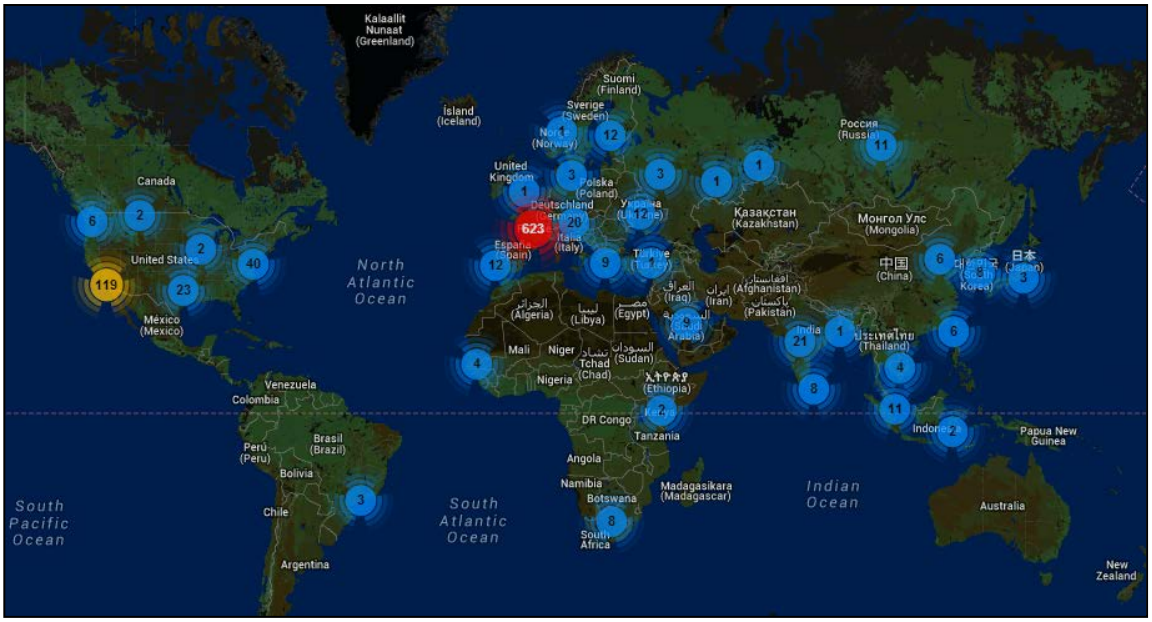


Abbildung 19 - Geographische Visualisierung mittels Splunk

[20] Vgl. https://apps.splunk.com/app/368/

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.4.1.3 File Share Analysis

Daten sind in vielen Unternehmungen, welche regelmässig mit der Datenverarbeitung zu tun haben vermutlich wertvollstes Gut und benötigen daher eines adäquaten Schutzes. Dennoch sind Logdaten oft nicht in einem verwertbaren Format oder die Logs werden schlichtweg nicht regelmässig kontrolliert.

Grundsätzlich gibt es die folgenden Ansätze zur Erkennung, ob ein missbräuchlicher Datenzugriff erfolgt:

- Anzahl der Zugriffe auf verschiedene Dateien pro Nutzer
  - Es ist äusserst unüblich, dass ein Benutzer auf viele verschiedene Dateien zugreift. Es ist eher der Fall, dass ein Benutzer immer mit den gleichen Daten arbeitet und sich daher die Gesamtzahl der Zugriffe auf einzelne Daten sich in einem sehr kleinen Bereich befindet.
- Geschwindigkeit der Zugriffe
  - Automatisierte Zugriffe können in einer viel schnelleren Zeitspanne erfolgen als manuelle. Im Fall, dass enorm viele Zugriffe erfolgen, kann davon ausgegangen werden, dass diese Zugriffe automatisiert erfolgt sind.
  - Die Schwierigkeit hierbei ist, dass diese Zugriffe durchaus auch legitimer Natur sein können. Das ist z.B. der Fall, wenn jemand einen ganzen Ordner vom Share herunterkopiert.
- Zugriffe zu ungewöhnlichen Zeiten (z.B. am Wochenende oder ausserhalb der Arbeitszeit)
  - Zugriffe ausserhalb der regulären Arbeitszeit sind ein Indiz für unzulässige automatisierte Zugriffe.
- Zugriffe auf bestimmte Dateien oder Ordner
  - Zugriffe auf bestimmte Dateien oder Ordner wie z.B. Abrechnungen sind relativ selten und können daher ein Indiz für Industriespionage darstellen.

Anzahl der Zugriffe auf verschiedene Dateien pro Nutzer

Mittels der nachfolgenden Suche kann ermittelt werden, wieviele Zugriffe auf verschiedene Dateien von einem einzelnen Nutzer erfolgt worden sind:

```
index=file_share action=read | dedup file_name user | top limit=20 user
```

In der nachfolgenden Abbildung sind zum Beispiel enorme Dateizugriffe seitens eines einzelnen Nutzers festzustellen:

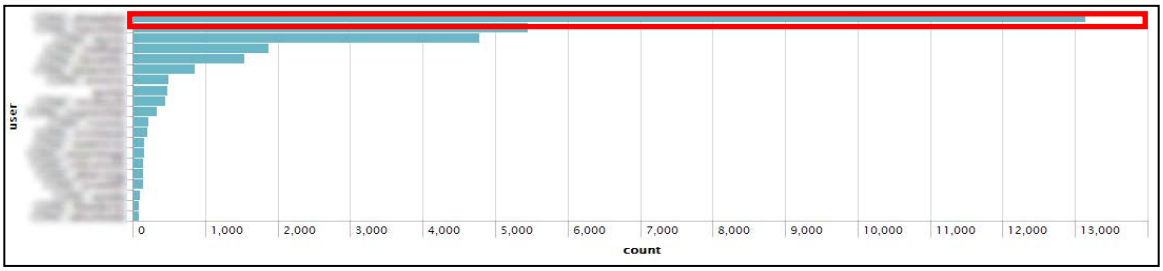


Abbildung 20 - Visualisierung der Dateizugriffe

Hier ist es jedoch wiederum äusserst wichtig, nicht zu vergessen, dass diese Ergebnisse keinesfalls in Stein gemeisselt sind. Diese Zugriffe könnten durchaus legitimer Natur sein (z.B. falls jemand eine grosse Anzahl von Dateien offline verfügbar machen will) und daher müssen all diese Fälle manuell verifiziert werden.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Dies ist durch die mächtige Funktionalität von Splunk relativ einfach. Es muss nur auf den betreffenden Benutzernamen geklickt werden, um anschliessend eine Liste der heruntergeladenen Dateien zu erhalten.

Geschwindigkeit der Zugriffe

Aufgrund der menschlichen Natur sind menschliche Zugriffe limitiert seitens der Geschwindigkeit. Ein Computerprogramm kann dagegen viel schneller agieren und wird dies in der Regel auch machen.

Mit der nachfolgenden Suchabfrage werden alle Zugriffe auf Dateien, welche innerhalb einer Zeitspanne von zehn Sekunden geschehen, gruppiert und anschliessend nach Anzahl zugegriffener Dateien herabsteigend sortiert.

```
index=file_share action=read | sort 0 user,_time | transaction user maxspan=10s
maxevents=-1 | search eventcount>10 | sort 0 -num(eventcount)
```

Zugriffe zu ungewöhnlichen Zeiten (nachts, etc.)

In einer Unternehmungsumgebung ist es äusserst unüblich, dass Dateizugriffe ausserhalb der normalen Bürozeiten erfolgen. Dies kann mit folgender Suchabfrage festgestellt werden.

```
index=file_share (date_hour>19 AND date_hour<7) | timechart count by user

index=file_share (date_wday=saturday OR date_wday=sunday) | timechart count by
user
```

Zugriffe auf bestimmte Dateien / Ordner

Im Falle von Daten geleakten Daten ist wünschenswert zu erfahren, von welchem Benutzer dies ausgegangen ist. Auch dies ist leicht zu eruieren.

```
index=file_share file_name="/data/internal/*" | dedup user file_name
```

6.4.1.4 Email Analysis

E-Mails sind ein beliebtes Kommunikationsmittel: Sie können zur legitimen Kommunikation als auch als Kommunikationskanal für illegitime Zwecke eingesetzt werden wie zum Beispiel zur Kontrolle von Botnetzen oder um Daten aus einer Unternehmung herauszuschmuggeln. Die folgenden Indizien sind hilfreich, um zu erkennen, ob unerwünschte Mails vorhanden sind:

- Grosse Mails an externe Nutzer
    - E-Mail sind eigentlich nicht zur Übertragung von grösseren Dateien gedacht. Dafür sind Protokolle wie FTP oder HTTP(S) vorgesehen. Eine grössere Ansammlung von grossen Mails an externe Parteien sollte daher eigentlich nicht passieren.
- Externe E-Mail Adressen, welche nur als Empfänger dienen
    - E-Mails werden oftmals zur bidirektionalen Kommunikation genutzt. Es ist äusserst selten, dass E-Mails an Gesprächspartner versendet werden, welche vorher noch nie eine Mail an diese Adresse gesendet haben.
- Erkennung von Zugriffen zu ungewöhnlichen Zeiten
    - Zugriffe ausserhalb der regulären Arbeitszeit oder am Wochenende können ein Indiz für unerlaubte Zugriffe darstellen.
    - Bei E-Mails muss jedoch daran gedacht werden, dass durch den zunehmenden BYOD-Trend die Arbeit oftmals auch mit nach Hause genommen wird und daher Zugriffe ausserhalb der Bürozeiten keine allzugrosse Besonderheiten mehr darstellen.
- Ausarbeitung einer Kontaktmatrix

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- Falls ein bestimmter Personenkreis in Verdacht ist, interne Informationen nach aussen kommuniziert zu haben, so kann die Visualisierung wer mit wem in Kontakt war äusserst hilfreich sein.

Mittels der nachfolgenden Suchbefehle können derartige Muster entdeckt werden:

Erkennung von grossen Mails an externe Nutzer

```
index=mails dst_user!="*@example.com" size>25
```

Erkennung von Mail Adressen, welche nur als Empfänger dienen (unidirektional)

```
index="mails" | sort 0 src_user,dst_user,_time | transaction dst_user dst_time
maxspan=-1 maxevents=-1 | search src_user != "*@example.com"
```

Erkennung von Zugriffen zu ungewöhnlichen Zeiten

```
index=mails (date_hour>19 AND date_hour<7) src_user="*@example.com" | timechart
count by src_user
index=mails (date_wday=saturday OR date_wday=sunday) src_user="*@example.com" |
timechart count by src_user
```

6.4.1.5 Firewall Logs

Firewalls stehen als Segmentierungselement zwischen zwei Zonen, mittels einer Analyse der Verbindungsdaten kann nachvollzogen werden ob unerlaubte Zugriffe auf andere interne Netze stattgefunden haben.

Die nachfolgenden Suchbefehle können dafür hilfreich sein:

Benutzung von vielen "High Ports"

```
index=firewall_logs NOT policy="drop" port>1000 | top limit=10000 port
```

Anzahl der Ports pro IP

```
index=firewall_logs NOT policy="drop" | chart count(port) by src_ip
```

6.4.1.6 SSH Logs

SSH ist ein Protokoll zur verschlüsselten Kommunikation mit einem entfernten Server. Die Hauptnutzung dafür ist die sichere Verwaltung von Servern über eine entfernte Kommandozeile.

Im Falle eines APT geht es darum, die Persistenz des Angriffes zu gewährleisten, selbst wenn ein befallenes System bereits erkannt wurde. Daher ist die Wahrscheinlichkeit, dass ein Angreifer via gestohlene Zugangsschlüssel oder simplen Bruteforce Angriffen versucht, Zugriffe auf weitere Systeme via SSH zu gewinnen nicht unwahrscheinlich. Die nachfolgenden Ansätze sind geeignet, um solche Zugriffe zu erkennen:

Loginversuche zwischen 19:00 und 07:00

```
index=authlog process=sshd (date_hour>19 AND date_hour<7) | timechart count by
user
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Loginversuche am Wochenende

```
index=authlog process=sshd (date_wday=saturday OR date_wday=sunday) | timechart
count by user
```

Fehlerhafte Loginversuche

```
index=authlog process=sshd state=Failed | timechart count by user

index=authlog process=sshd state=Failed | timechart count by src_ip
```

Liste der IP Adressen pro Benutzer

```
index=authlog process=sshd | chart count(src_ip) by user
```

6.4.2 Auschluss von good known/bad known Hosts

Falls die Suche nach Anomalien keinerlei aufschlussreiche Ergebnisse liefert, ist es sinnvoll, die Verbindungen in "Bad known" und "God known" Hosts aufzuteilen.

Dies setzt voraus, dass jegliche Verbindungen geloggt werden und so eine Analyse möglich ist. Am besten lässt sich dies über die Logdaten von zentralen Firewalls verwirklichen.

Um Verbindungen als gut- oder bösartig darzustellen ist es erstmal von Nöten, die als gutartig bekannten Hosts zu definieren, in einer CSV Datei festzuhalten und dann als Inputlookup festzulegen. Ein Beispiel kann nachfolgend angesehen werden:

```
dst_ip
225.167.240.162
229.8.15.201
[CUT BY COMPASS]
```

Falls jeweils nur die Verbindungen von einzelnen Systemen gefiltert werden sollen, kann auch eine Source IP festgelegt werden. Im folgenden Beispiel sind die Verbindungen von 192.168.1.123 nach 225.167.240.162 sowie 192.168.1.32 nach 229.8.15.201 erlaubt.

```
src_ip,dst_ip
192.168.1.123,225.167.240.162
192.168.1.32,229.8.15.201
[CUT BY COMPASS]
```

Anschliessend kann folgende Suche genutzt werden, um alle Verbindungen anzuzeigen, welche als nicht vertrauenswürdig eingestuft wurden:

```
index="firewall" NOT [inputlookup good_known_host ]
```

Die Liste der als vertrauenswürdig eingestuften Adressen kann selbstverständlich laufend ergänzt werden, um die Liste der potentiell bösartigen Systeme weiter einzugrenzen.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.4.3 Visualisierungen

Ein Bild sagt bekanntlich mehr als tausend Worte und dies ist auch bei der Analyse von Logdaten von äusserster Wichtigkeit. Mittels Visualisierungen können beispielsweise Beziehungsnetzwerke ("Welcher Host hatte Verbindungen zum fraglichen System") oder zeitliche Veränderungen ("Wann ist das passiert?") leichter verarbeitet werden.

Vorallem die OpenSource Software "Gephi"[21] kann in Verbindung mit Splunk hervorragend genutzt werden, um Verbindungen zu visualisieren. Ein Ergebnis einer solchen Visualisierung ist in Abbildung 23 zu sehen.

Um Daten zu visualisieren sind die folgenden Schritte notwendig:

1. Import des Datensets in Splunk

2. Filterung der gewünschten Einträge und Definition, welche Felder exportiert werden sollen:
   `index=firewall | fields src_ip dst_ip`

3. Export zu CSV

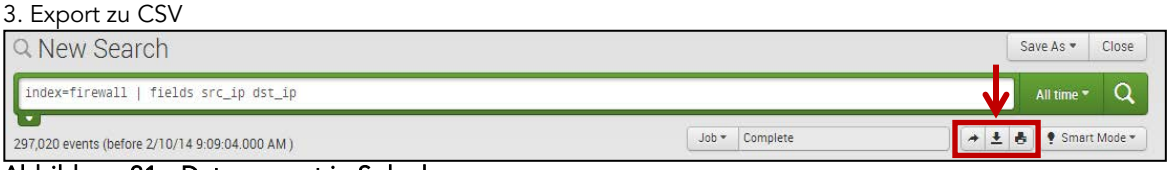


Abbildung 21 - Datenexport in Splunk

4. Alle Datenfelder ausser "src_ip" und "dst_ip" sollten aus der CSV Datei gelöscht werden. Das Feld "src_ip" muss in "source" und "dst_ip" in "destination" umgewandelt werden.

5. In Gephi kann die Datei nun mit folgenden Schritten importiert werden.
   1. "Data Laboratory"
   2. Import Spreadsheet
   3. As table → Edge Table

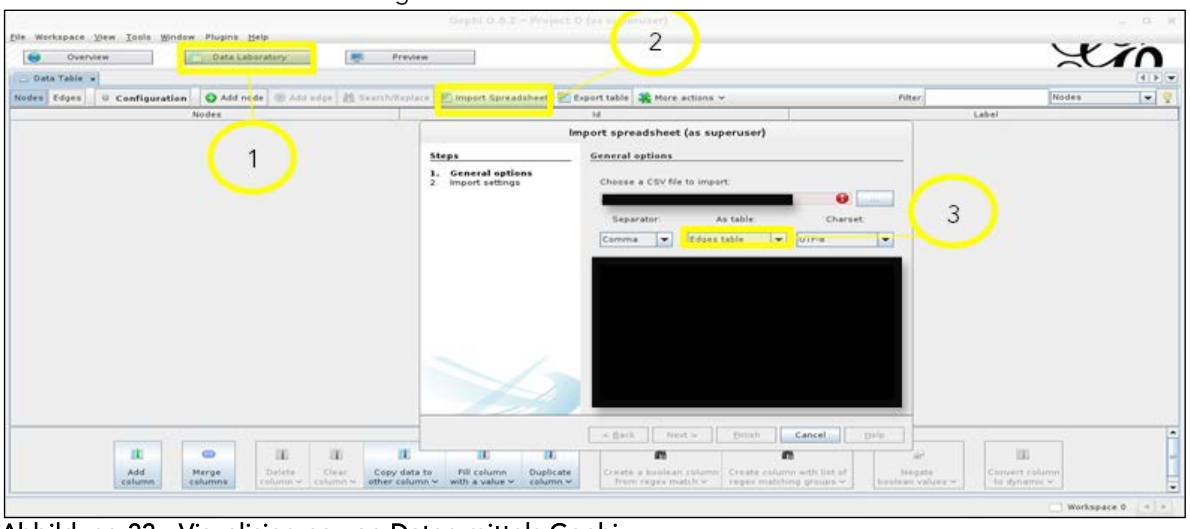


Abbildung 22 - Visualisierung von Daten mittels Gephi

[21] https://gephi.org

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Nach dem Import visualisiert Gephi nun alle Verbindungen. Dies kann je nach Anzahl der betroffenen Systeme durchaus einige Stunden in Anspruch nehmen. In der nachfolgenden Abbildung 23 sind die Verbindungen eines kleineren Netzwerkes visualisiert:

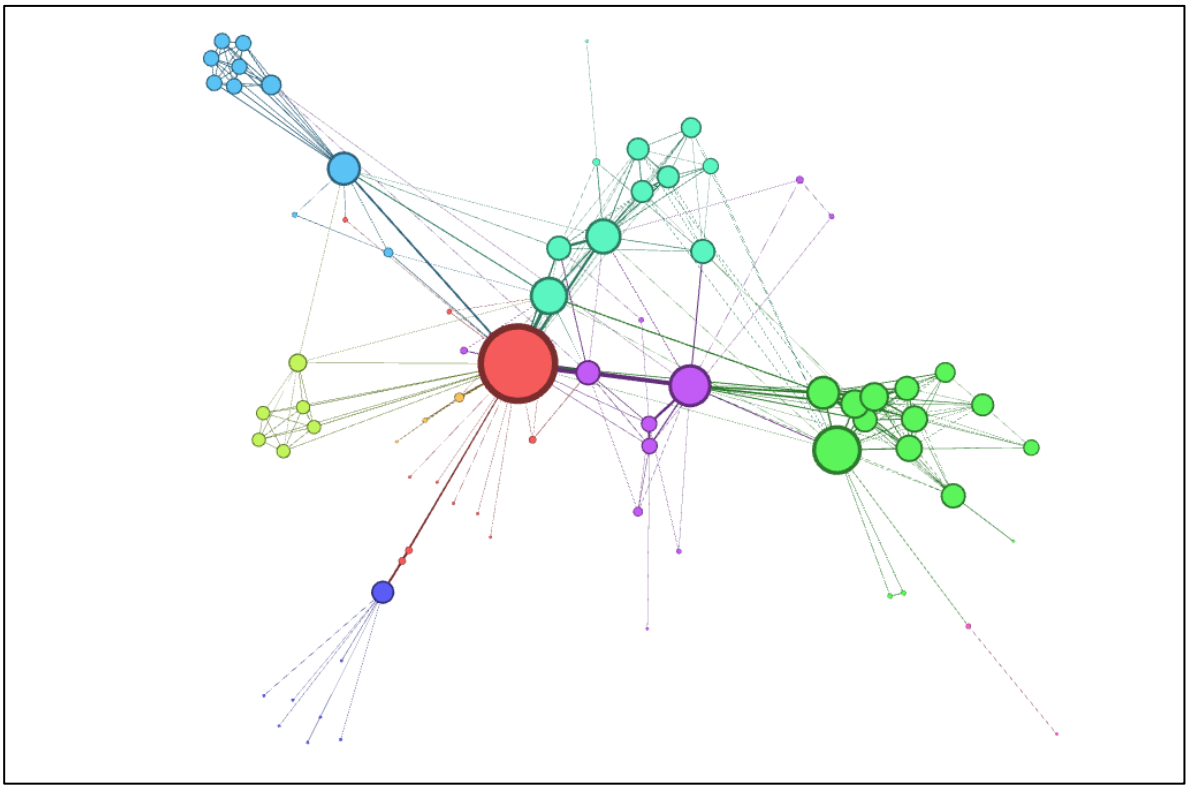


Abbildung 23 - Verbindungen zwischen einzelnen Hosts visualisiert

In der obigen Abbildung lassen sich keine grösseren Anomalien feststellen. Die einzelnen Hosts welche mit externen Systemen aufnehmen agieren als DNS- oder Domänenserver.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7 Loggingempfehlungen

Um Logs von verschiedenen Applikationen und Geräten adäquat miteinander vergleichen zu können, ist es wichtig, die Daten in einem möglichst konsistenten Format abzuspeichern. Eine Vergleichbarkeit ist nur gewährleistet, wenn die Datenfelder immer gleich benannt sind. Daher wird im Folgenden konsequent auf die nachfolgenden Typen gesetzt:

Typ	Feldname
IP Adresse des Absenders	src_ip
IP Adresse des Empfängers	dst_ip
Domain des Absenders	src_domain
Domain des Empfängers	dst_domain
Identifier	identifier
Username	user

Einzelne themenbezogene Felder (z.B. den Typ der DNS Abfrage) werden in den nachfolgenden Kapiteln einzeln behandelt.

7.1 OpenSSH

OpenSSH ist mit über 80% Marktanteil mit Abstand der am meisten genutzte SSH Server.[22] Die Standardeinstellungen des SSH Dämons variieren je nach eingesetzter Distribution und sollten daher manuell überprüft werden. Oftmals wird nur der LogLevel "INFO" gesetzt, bei diesem werden fehlerhafte Loginversuche aber nicht dokumentiert.

Um ein optimales Logging zu gewährleisten, sollten die folgenden Einstellungen gesetzt werden:

```
root@dns:/var/# cat /etc/ssh/sshd_config

[CUT BY COMPASS]
LogLevel VERBOSE
SysLogFacility AUTH
[CUT BY COMPASS]
```

Zusätzlich müssen die folgenden Felder definiert werden:

```
root@splunk: /# cat /opt/splunk/etc/system/local/props.conf

[CUT BY COMPASS]
[sshd]

.*? sshd\[([0-9]+)\]: (Accepted|Failed) (password|publickey) for ([^ ])+ from
(?P<src_ip>\d+\.\d+\.\d+\.\d+) port ([0-9]+) ssh2
```

[22] Vgl. http://www.openssh.com/usage/graphs.html

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
.*? sshd\[([0-9]+)\]: (Accepted|Failed) (password|publickey) for (?P<user>[^ ]+)
from (\d+\.\d+\.\d+\.\d+) port ([0-9]+) ssh2
.*? sshd\[([0-9]+)\]: (?P<state>(Accepted|Failed)) (password|publickey) for ([^
]+) from (\d+\.\d+\.\d+\.\d+) port ([0-9]+) ssh2
```

7.2 Mail

Die folgenden Feldtypen werden zusätzlich genutzt:

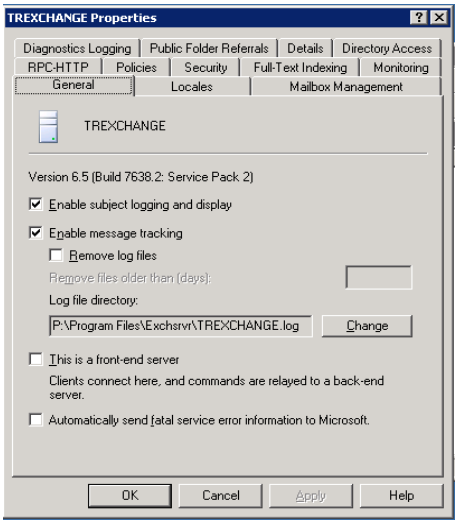
Typ	Feldname
Betreff	subject
Grösse	size

7.2.1 Exchange Server 2003

Exchange 2003 loggt in den Standardeinstellungen nur unzureichend. Um auswertbare Logs zu erhalten ist es notwendig, die folgenden Aktionen durchzuführen:

1. Aufruf von *"Exchange System Manager.msc"* (mit Anführungszeichen)
2. Auswahl des betreffenden Servers und Rechtsklick auf *Properties*
3. Auswahl des Reiters *General*

Compass empfiehlt die folgenden Einstellungen um auswertbare Ergebnisse zu erhalten:



- Enable subject logging and display
- Enable message tracking

Abbildung 24 - Exchange 2003 Logeinstellungen

Die Exchange Logs werden nun in dem unter *Log file directory* spezifizierten Ordner abgespeichert. Jeden Tag wird dabei eine neue Logdatei angelegt.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.3 DNS

Die folgenden Feldtypen werden zusätzlich genutzt:

Typ	Feldname
DNS Abfrage Typ (MX/A/etc…)	type
Top-Level Domain (z.B. "ch")	dst_tld
Second-Level (z.B. "csnc")	dst_sld
Subdomains (z.B. "www")	dst_subdomain

7.3.1 BIND9

Export

Das Logging von DNS Anfragen muss erst in der */etc/named.conf* konfiguriert werden. Die folgenden Einstellungen werden empfohlen, um jegliche DNS Anfragen zu loggen:

```
root@dns:/var/# cat /etc/named.conf

[CUT BY COMPASS]
logging {
       channel "dns_queries" {
                file "/var/log/queries.log" versions 4 size 100m;
                print-time yes;
                severity debug;
        };


        category "queries" { "dns_queries"; };
};
[CUT BY COMPASS]
```

Die Logs werden nun in */var/log/queries.log* abgelegt.

Import

Date	Time		Remote IP	Port		Name		Type
05-Feb-2014	10:12:51.932	client	76.72.173.158	#42158:	query:	168.160-190.178.254.212.in-addr.arpa	IN	PTR

Das folgende Regelsets kann für den Import von BIND9 Logs genutzt werden:

```
root@splunk: /# cat /opt/splunk/etc/system/local/props.conf

[CUT BY COMPASS]
[bind9]

# Every entry is on a new line
SHOULD_LINEMERGE=false
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
# Define timestamp format
TIME_FORMAT = %d-%b-%Y %H:%M:%S.%L

# Extract whole domain name
EXTRACT-bind9_dst_domain = (?i) query: (?P<dst_domain>[^ ]+)

# Extract top level domain
EXTRACT-bind9_dst_tld = (?i)\..*?\.(?P<dst_tld>\w+)(?= )

# Extract second level domain
EXTRACT-bind9_dst_sld = (?i) query: (([a-zA-Z0-9_\-]+\.)?)+(?P<dst_sld>[^
]+)(?=\.)

# Extract all subdomains
EXTRACT-bind9_dst_subdomain = (?i) .*?: (?P<dst_subdomain>[^ ]+)(?=\.)[^ ]+\.

# Extract remote IP
EXTRACT-bind9_src_ip = (?i) client (?P<src_ip>[^#]+)

# Extract type
EXTRACT-bind9_type = (?i) IN (?P<type>[^ ]+)

# Show in pull down
pulldown_type = 1

[CUT BY COMPASS]
```

7.3.2 Windows Server 2003 DNS Server

Export

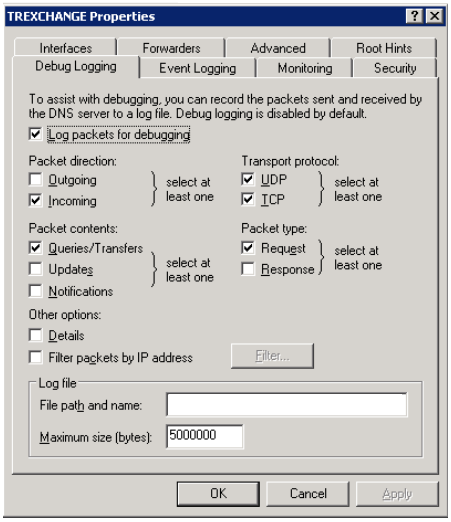
Windows Server 2003 loggt in den Standardeinstellungen keinerlei DNS Anfragen. Um auswertbare Logs zu erhalten, ist es notwendig die DNS Debug Logs zu aktivieren:

4. Aufruf von *dnsmgmt.msc /s*
5. Auswahl des betreffenden DNS Servers und Rechtsklick auf *Properties*
6. Auswahl des Reiters *Debug Logging*
7. Ankreuzen der Checkbox *Log packets for debugging*

Compass empfiehlt die folgenden Einstellungen, um auswertbare Ergebnisse zu erhalten:

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch



- Packet direction: Incoming
- Transport protocol: UDP, TCP
- Packet contents: Queries/Transfers
- Packet type: Request

Abbildung 25 - DNS Server Logeinstellungen unter Windows Server 2003

Die DNS Anfragen werden nun in der Datei *C:\WINDOWS\system32\dns\dns.log* abgespeichert.

Import

Die Daten werden in einem menschenlesbaren Textformat gespeichert. Im nachfolgenden Beispiel **Error! Reference source not found.**werden die für eine Analyse benötigten Bestandteile aufgegliedert.

```
Date      Time              ID                Remote IP                                  Type
20140204  15:53:51 818 PACKET  02ABB480 UDP Rcv 192.168.100.50  a235   Q [0001   D   NOERROR]  PTR
(2)14(3)102(3)168(3)192(7)in-addr(4)arpa(0)
                    Name
```

Das folgende Regelset kann für den Import von Windows 2003 DNS Logs genutzt werden:

```
root@splunk: /# cat /opt/splunk/etc/system/local/props.conf

[CUT BY COMPASS]
[win03_dns]
# Replace numbers in name with .
SEDCMD-win03_dns = s/\(\d+\)/./g

# Every entry is on a new line
SHOULD_LINEMERGE=false

# Define timestamp format
TIME_FORMAT = %Y%m%d %H:%M:%S

# Extract name
EXTRACT-win03_dns_dst_domain = .*? \.(?P<dst_domain>([a-zA-Z_.\-0-9]+))\.

# Extract identifier
EXTRACT-win03_dns_identifier = (?i) [A-Z]+ (?P<identifier>[^ ]+)
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
# Extract remote IP
EXTRACT-win03_dns_src_ip = (?i) (Rcv|Snd) (?P<src_ip>[^ ]+)

# Extract type
EXTRACT-win03_dns_type = (?i) .*?\] (?P<dns_type>\w+)(?= )

# Show in pull down
pulldown_type = 1

[CUT BY COMPASS]
```

7.4 Web

Die folgenden Feldtypen werden zusätzlich genutzt:

Typ	Feldname
Byte	byte
Method	method
Parameter	parameter
Referer	referer
Statuscode	status_code
Type	type
URL	url
User Agent	user_agent

7.4.1 squid

Export

Squid terminiert in den Standardeinstellungen keine verschlüsselten HTTPS Verbindungen. Dies kann mittels der Direktive "ssl_bump" aktiviert werden. Viele Distributionen haben Squid ohne *--enable-useragent-log* kompiliert, in diesen Fällen sollte die Software selbst kompiliert werden. Eine Anleitung für die gängisten Systeme ist unter http://wiki.squid-cache.org/SquidFaq/CompilingSquid verfügbar.

```
root@splunk: /# cat /etc/squid/squid.conf

[CUT BY COMPASS]
# Listen on port 3128 and configure SSL certificates
http_port 3128 ssl-bump generate-host-certificates=on
dynamic_cert_mem_cache_size=4MB cert=/usr/local/squid/ssl_cert/myCA.pem

# Enable access log with combined squid format
# combined squid format does also log user agent and referer
access_log /var/log/squid/access.log combined
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
# Forward any request
always_direct allow all

# Enable SSL bumping
ssl_bump allow all

# Log query parameters
strip_query_terms off
[CUT BY COMPASS]
```

Die Logs werden dann unter "/var/log/squid/access.log" abgelegt.

Import

Die Daten werden in einem menschenlesbaren Textformat gespeichert.

Time		Src. IP	Code	SC	Byte	Method	URL		
1392027472.366	135	212.254.178.163	TCP_MISS/	200	5954	GET	http://www.wikipedia.de/style.css	-	DIRECT/
195.10.208.211	text/css								
Dst. IP	Type								

Das folgende Regelset kann für den Import von nativ gespeicherten squid Logs genutzt werden:

```
root@splunk: /# cat /opt/splunk/etc/system/local/props.conf

[CUT BY COMPASS]
[squid_access]

# Every entry is on a new line
SHOULD_LINEMERGE=false

# Define timestamp format
TIME_FORMAT=%d/%b/%Y:%I:%M%S %z

# Extract source IP
EXTRACT-squid_access_src_ip = (?i)^(?P<src_ip>[^ ]+)

# Extract user agent
EXTRACT-squid_access_user_agent = (?i)^(?:[^ ]* ){11}"(?P<user_agent>[^"]+)"

# Extract referer
EXTRACT-squid_access_referer = (?i)^(?:[^ ]* ){10}"(?P<referer>[^ ]+)"

# Extract status code
EXTRACT-squid_access_status_code = (?i)^(?:[^ ]* ){8}(?P<status_code>[^ ]+)

# Extract byte
EXTRACT-squid_access_byte = (?i)^(?:[^ ]* ){9}(?P<byte>[^ ]+)

# Extract method
EXTRACT-squid_access_method = (?i)^[^\+]*\+\d+\]\s+"(?P<method>[^ ]+)

# Extract URL
EXTRACT-squid_access_url =
(?i)"(GET|HEAD|POST|PUT|DELETE|TRACE|OPTIONS|CONNECT|PATCH) (?P<url>[^ ?]+)

# Extract parameter
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
EXTRACT-squid_access_parameter = (?i)^(?:[^\.]*\.){5}[a-zA-Z._\-/0-
9]+\?(?P<parameter>[^ ]+)

# Extract dst_domain
EXTRACT-squid_access_dst_domain = (?i)(http(s)?://|CONNECT
)(?P<dst_domain>[^/:]+)

# Extract dst_ip
EXTRACT-squid_access_dst_ip = (?i):[A-Z_]+ (?P<dst_ip>[^ ]+)

# Extract type
EXTRACT-squid_access_type = (?i):[A-Z_]+ [0-9\.]+ (?P<type>[^ ]+)

# Show in pull down
pulldown_type = 1

[CUT BY COMPASS]
```

7.5 FTP

Die folgenden Feldtypen werden zusätzlich genutzt:

Typ	Feldname
Typ des Zugriffes	action
Dateigrösse	file_size
Dateiname	file_name

7.6 Firewall

Die folgenden Feldtypen werden zusätzlich genutzt:

Typ	Feldname
Port	port
Policy	policy

7.7 Dateizugriffe

Die folgenden Feldtypen werden zusätzlich genutzt:

Typ	Feldname
Typ des Zugriffes	action
Dateigrösse	file_size

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Typ	Feldname
Dateiname	file_name

7.7.1 Synology DSM 4

Export

Synology NAS loggen standardmässig keine Dateizugriffe. Das Logging muss über das Webinterface aktiviert werden: *Control Panel -> Win/Mac/NFS -> Windows File Service -> Enable Transfer Log*

Die Logs können dann als CSV via *Systemlogs -> File Transfer -> Windowsfile transfer* exportiert werden.

Import

Das folgende Regelset kann für den Import von Synology DSM Logs genutzt werden:

```
[dsm4_smb_transfer]

# Every entry is on a new line
SHOULD_LINEMERGE=false

# Define timestamp format
TIME_PREFIX=,
TIME_FORMAT=%Y/%m/%d %H:%M:%S

# Extract remote IP
EXTRACT-dsm4_smb_transfer_src_ip = (?i)^(?:[^,]*,){2}(?P<src_ip>[^,]+)

# Extract user
EXTRACT-dsm4_smb_transfer_user = (?i)^(?:[^,]*,){3}(?P<user>[^,]+)

# Extract action
EXTRACT-dsm4_smb_transfer_action = (?i)^(?:[^,]*,){4}(?P<action>[^,]+)

# Extract type
EXTRACT-dsm4_smb_transfer_type = (?i)^(?:[^,]*,){5}(?P<type>[^,]+)

# Extract file size
EXTRACT-dsm4_smb_transfer_file_size = (?i)^(?:[^,]*,){6}(?P<file_size>[^,]+)

# Extract file name
EXTRACT-dsm4_smb_transfer_file_name = (?i)^(?:[^,]*,){7}(?P<file_name>[^,]+)

# Show in pull down
pulldown_type = 1
```


Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

8 Schlusswort

Zwar konnte im Rahmen dieses Whitepapers kein Allheilmittel gegen Advanced Persistent Threats erarbeitet werden. Trotzdem bin ich mit den Ergebnissen zufrieden. Denn die Vielfalt der möglichen Angriffsszenarien und Angriffsmethodiken ist schlichtweg zu gross für eine allgemeingültige Lösung. Eine halbautomatisierte Lösung ist meines Erachtens nach die beste Methode zur Analyse von APTs.

Der Trend, dass immer mehr Daten mittels elektronischer Datenverarbeitung verarbeitet werden wird sich, meiner Auffassung nach, weiter so fortsetzen. Eine Welt ohne elektronische Datenverarbeitung ist heute beinahe unvorstellbar. Auch Regierungen und Kriminelle sind nicht in der Zeit stehengeblieben und werden auch diese Möglichkeit nutzen, um an Informationen jeglicher Art zu gelangen. So ist ein Zeichen der Zeit, dass gerade in die Fertigstellungswoche dieses Whitepapers die kritische Schwachstelle Heartbleed für Aufregung sorgte.

Die Kernfrage ist daher nicht mehr, *ob* ein Netzwerk sicher ist, sondern *wie* sicher es ist. Es ist unrealistisch zu glauben, dass es für einem Angreifer mit beinahe unbegrenzten Ressourcen unmöglich ist, ein Netzwerk erfolgreich zu infiltrieren. Aber viele Angreifer besitzen solche Möglichkeiten nicht, und diese diese Angriffe können effektiv verhindert werden.

8.1 Einschränkungen

Die im Rahmen dieses Whitepapers erarbeiteten Vorschläge unterliegen verständlichermassen auch einigen Restriktionen. Zu diesen Problematiken gehören unter anderem die folgenden Punkte:

- Die Lizenzkosten von Splunk bemessen sich anhand der täglich zu indexierenden Datenmenge.
    - In der kostenlosen Community-Version sowie der preiswertesten kostenpflichtigen Version lassen sich pro Tag nur 500 Megabyte an Daten importieren. Bei Datensets von mehreren Gigabyte dauern Importe entsprechend länger.
- Die Indexierungs- und Suchgeschwindigkeit korreliert mit der Geschwindigkeit der eingesetzten Hardware.
    - Die Nutzung von schneller und aktueller Hardware ist zwingend notwendig, um die Ergebnisse innert einer adäquaten Zeitphase zu erhalten.

8.2 Verbleibende Arbeiten / Ausblick

Erstmals gilt es die in diesem Dokument vorgeschlagenen und erarbeiteten Suchbefehle und Heuristiken anhand mehrer Kundenprojekte zu verifizieren und in einem realen Netzwerk auszuprobieren. Im Rahmen dieser Analysen sind unter anderem die folgenden Arbeiten denkbar:

- Erarbeitung weiterer Suchbefehle und Heuristiken,
- Erarbeitung weiterer Anleitungen und regulärer Ausdrücke für den Export von Logdaten.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

9 Appendix

9.1 Abbildungsverzeichnis

9.2 Tabellenverzeichnis

9.3 Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik. (2006). Remote-Controlled Browsers System (ReCoBS) - Grundlagen und Anforderungen. Bonn, Deutschland. Von BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf abgerufen am 10. April 2014

Carasso, D. (2012). *Exploring Splunk - Search processing language (SPL) primer and cookbook.* New York: CITO Research.

Cole, E. (2012). *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Syngress.

Editor, R. (kein Datum). RFC 2616. *Internet Requests for Comment.* The IETF Trust.

FireEye. (2013). *Advanced Threat Report – 2H 2012.* Von http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf abgerufen am 10. April 2014

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Fortinet. (2013). *Threats on the Horizon: The Rise of the Advanced Persistent Threat.* Von http://www.fortinet.com/sites/default/files/solutionbrief/threats-on-the-horizon-rise-of-advanced-persistent-threats.pdf abgerufen am 10. April 2014

Gregory, P. (2013). *Advanced Persistent Threat Protection for Dummies.* New Jersey: John Wiley & Sons, Inc.

Himmelein, G. (11. November 2013). *Supertrojaner BadBIOS: Unwahrscheinlich, aber möglich*. Von http://heise.de/-2043114 abgerufen am 10. April 2014

ISACA. (2013). *Advanced Persistent Threat Awareness - Study Results.* Von http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/wp_apt-survey-report.pdf abgerufen am 10. April 2014

Kamkar, S. (2012). How I Met Your Girlfriend: The discovery and execution of entirely new classes of Web attacks in order to meet your girlfriend. Von http://samy.pl/talks/2010-talk.ppt abgerufen am 10. April 2014

Katsuki, T. (16. November 2012). *Malware Targeting Windows 8 Uses Google Docs.* Von http://www.symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs abgerufen am 10. April 2014

Kornblum, J. (2006). Identifying almost identical files using context triggered piecewise hashing. *digital investigation 3*, 91-97.

Krebs, B. (21. June 2012). *Krebs on Security.* Von A Closer Look: Email-Based Malware Attacks: http://krebsonsecurity.com/2012/06/a-closer-look-recent-email-based-malware-attacks/ abgerufen am 10. April 2014

Lewis, T. (24. December 2013). *HTTP header heuristics for malware detection.* Von https://www.sans.org/reading-room/whitepapers/detection/http-header-heuristics-malware-detection-34460 abgerufen am 10. April 2014

Mandiant. (2010). *M-Trends - The advanced persistent threat.*

Mandiant. (2012). *M-Trends - An evolving threat.* Von https://www.mandiant.com/resources/mandiant-reports/ abgerufen am 10. April 2014

Mandiant. (2013). *APT1 - Exposing One of China's Cyber Espionage Units.*

Mandiant. (2013). *M-Trends - Attack the Security Gap™.*

Sourcefire VRT Labs. (kein Datum). *Zeus Trojan Analysis.* Von https://labs.snort.org/papers/zeus.html abgerufen am 10. April 2014

Splunk Inc. (2013). *Search Manual.* Von http://docs.splunk.com/Documentation/Splunk/latest/Search/WhatsInThisManual abgerufen am 10. April 2014

Splunk Inc. (2013). *Search Reference.* Von http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/WhatsInThisManual abgerufen am 10. April 2014

Splunk Inc. (kein Datum). *Search Reference > anomalies.* Von http://docs.splunk.com/Documentation/Splunk/6.0.1/SearchReference/Anomalies abgerufen am 10. April 2014

Splunk Inc. (kein Datum). *Splunk License Comparison Table.* Von http://www.splunk.com/view/free-vs-enterprise/SP-CAAAE8W abgerufen am 10. April 2014

Strobel, S. (February 2014). Technische Ansätze zum Schutz vor APTs. *iX – Magazin für professionelle Informationstechnik*, S. 109 - 111.

Websense Inc. (2011). *Advanced persistent threats and other advanced attacks: Threat analysis and defense.* Von http://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf abgerufen am 10. April 2014

White, T. (2012). *Hadoop: The Definitive Guide* (3rd Ausg.). O'Reilly Media.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

9.4 Training

Möchten Sie gerne mehr zum Thema wissen und möchten Sie auch erfahren, was dies in der Praxis bedeutet, dann können wir Ihnen wärmstens unser nächstes "Hands-on Seminar" mit dem Titel: Network Analysis & Advanced Persistent Threats vom 25. und 26. August 2015 in Bern empfehlen.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch