Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Datenabfluss im Falle von Dateiprüfungen bei VirusTotal

CSW-Nr. 2022-206270-1032, Version 1.0, 15.03.2022

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

VirusTotal ist ein vom Unternehmen Google Inc. betriebener kostenloser Online-Dienst, bei dem man einzelne Dateien hochladen kann, die dann online durch aktuell über 70 verschiedene Antivirenprogramme und Malwarescanner überprüft werden. Dieser Dienst wird von Privatpersonen und Unternehmen oftmals zur Prüfung von verdächtigen Dateien genutzt, um aufgrund der Vielzahl von Antivirenprogrammen verlässlichere Ergebnisse als mit nur einem Scanner zu erhalten.

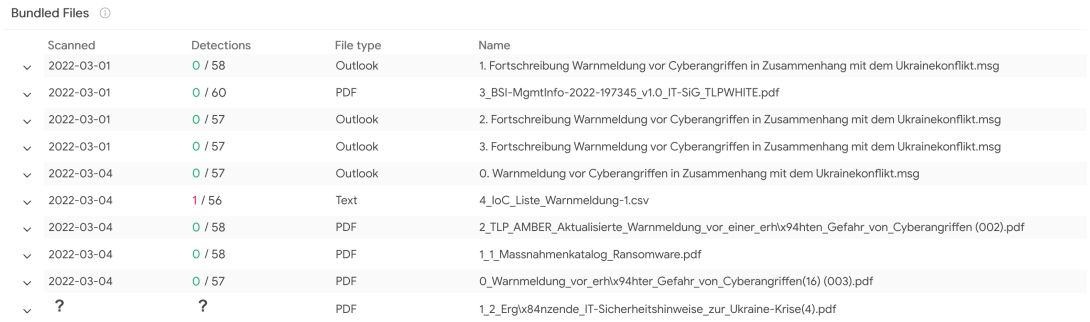
VirusTotal bietet diverse Services an, z.B. VirusTotal Intelligence oder VT Enterprise, bei denen man als Kunde Zugriff auf alle beim Online-Dienst hochgeladenen Dateien Dritter erhält. Zu den Kunden dieser Services gehören neben IT-(Security) Dienstleistern auch weitere Unternehmen, Geheimdienste, Forscher und Journalisten.

Im Rahmen eines Vorfalls wurde entdeckt, dass in einer Institution regelmäßig verdächtige E-Mail Anhänge, die in die Quarantäne verschoben werden, teil-automatisiert zu VirusTotal hochgeladen werden. Bei den verdächtigen Dateien handelte es sich in Einzelfällen um vertrauliche interne Dokumente. Die Inhalte dieser Dateien müssen als abgeflossen angesehen werden.

Das BSI stellt darüber hinaus fest, dass vereinzelt auch BSI Cyber-Sicherheitswarnungen und Lageberichte mit TLP:GREEN- oder TLP:AMBER-Markierung von Empfängern bei VirusTotal hochgeladen werden, siehe

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

beigefügten Screenshot. Bei einzelnen Empfängern besteht der Verdacht, dass die Dokumente automatisch an VirusTotal hochgeladen werden.



Bundled Files

Scanned	Detections	File type	Name
2022-03-01	0 / 58	Outlook	1. Fortschreibung Warnmeldung vor Cyberangriffen in Zusammenhang mit dem Ukrainekonflikt.msg
2022-03-01	0 / 60	PDF	3_BSI-MgmtInfo-2022-197345_v1.0_IT-SiG_TLPWHITE.pdf
2022-03-01	0 / 57	Outlook	2. Fortschreibung Warnmeldung vor Cyberangriffen in Zusammenhang mit dem Ukrainekonflikt.msg
2022-03-01	0 / 57	Outlook	3. Fortschreibung Warnmeldung vor Cyberangriffen in Zusammenhang mit dem Ukrainekonflikt.msg
2022-03-04	0 / 57	Outlook	0. Warnmeldung vor Cyberangriffen in Zusammenhang mit dem Ukrainekonflikt.msg
2022-03-04	1 / 56	Text	4_IoC_Liste_Warnmeldung-1.csv
2022-03-04	0 / 58	PDF	2_TLP_AMBER_Aktualisierte_Warnmeldung_vor_einer_erh\x94hten_Gefahr_von_Cyberangriffen (002).pdf
2022-03-04	0 / 58	PDF	1_1_Massnahmenkatalog_Ransomware.pdf
2022-03-04	0 / 57	PDF	0_Warnmeldung_vor_erh\x94hter_Gefahr_von_Cyberangriffen(16) (003).pdf
?	?	PDF	1_2_Erg\x84nzende_IT-Sicherheitshinweise_zur_Ukraine-Krise(4).pdf

Abb. 1: Screenshot: Geleakte BSI Warnmeldungen auf VirusTotal

Bewertung

Während die Prüfung von Datei-Hashwerten auf VirusTotal grundsätzlich unkritisch ist, kann der Upload von verdächtigen Dateien problematisch sein: Beim Upload von verdächtigen Dateien zu Virustotal gibt man die Vertraulichkeit der hochgeladenen Dateien auf und macht diese, aufgrund der Vielzahl und Diversität der VirusTotal-Kunden mit Zugriff auf die hochgeladenen Dateien, de facto öffentlich verfügbar. Man stimmt dieser Datenweitergabe an Dritte mit den Nutzungsbedingungen auch explizit zu. Neben den Kunden können auch alle der über 70 Antivirenhersteller eine Kopie der hochgeladenen Datei erhalten. Viele der AV-Hersteller haben ihren Sitz außerhalb der EU und verarbeiten die Daten auch außerhalb der EU.

Es ist davon auszugehen, dass weltweit Institutionen hochgeladene Dateien im Rahmen von (Wirtschafts-)Spionage auswerten und Filter für Stichwörter, beispielsweise "Verschlusssache" oder "Intern", gesetzt haben, wodurch sie in Echtzeit bei einem Upload solcher Dokumente informiert werden. Oft erfolgt ein Download dieser Dokumente dann automatisiert.

Die Auswirkungen auf die Vertraulichkeit durch einen Upload und die daraus entstehenden Konsequenzen sind den Mitarbeitenden innerhalb der Institution oftmals nicht bekannt.

Durch den Upload von TLP-markierten BSI-Warnungen schaden die Uploader dem Ansehen des Verteilkreises und des BSI. Das BSI muss in solchen Fällen prüfen, ob es mit betroffenen Verteilkreisen noch alle Informationen teilen kann oder zum Schutz der Vertraulichkeit von Informationen ggf. einzelne Sachverhalte, Hinweise und IOCs zurückhalten muss.

Mögliche Auswirkungen auf Kritische Infrastrukturen inkl. Verwaltung

Der geschilderte Vorfall kann in ähnlicher Art auch die Verwaltung und Kritische Infrastrukturen treffen und die dargestellten Konsequenzen haben.

- Ein Upload eines gemäß **Verschlusssachenanweisung (VSA)** eingestuften Dokumentes auf VirusTotal stellt einen **meldepflichtigen Verstoß gegen die Geheimhaltungspflicht** dar. Der zuständige Geheimschutzbeauftragte ist unverzüglich zu informieren. Es drohen disziplinar- oder arbeitsrechtliche Maßnahmen und eine strafrechtliche Ahndung des Verstoßes. Aus Verstößen gegen die VSA kann sich weiterhin die Ungeeignetheit von Personen zur Arbeit mit Verschlusssachen ergeben. Konsequenz ist der Ausschluss von der Bearbeitung von Verschlusssachen.
- Ein Upload eines Dokumentes mit personenbezogen Daten ist eine **Verletzung des Schutzes personenbezogener Daten**, die gemäß **DS-GVO meldepflichtig** ist. Der Vorfall ist wie ein Leak dieses Dokumentes zu behandeln und innerhalb der gesetzlichen Meldefristen an die Datenschutz-Aufsichtsbehörde zu melden. Hierzu ist der

zuständige behördliche bzw. betriebliche Datenschutzbeauftragte unverzüglich zu informieren. Verstöße können insbesondere mit empfindlichen Bußgeldern geahndet werden.

- Ein Upload eines Dokuments mit TLP:GREEN, TLP:AMBER oder TLP:RED Markierung auf VirusTotal stellt einen **Verstoß gegen die Traffic Light Protokoll (TLP) Verpflichtung** dar und kann zum Ausschluss aus dem jeweiligen TLP-Verteilkreis führen.
- Allgemein bedeutet ein Upload eines Dokumentes auf VirusTotal den **Verlust der Vertraulichkeit** der Inhalte. Hochgeladene Informationen müssen de facto als öffentlich angesehen werden.

In manchen Fällen verweigert VirusTotal Löschanfragen von fälschlicherweise hochgeladenen Dateien. Selbst wenn ein Dokument im Nachhinein doch gelöscht werden kann, sind die Inhalte aufgrund der Möglichkeit von Echtzeit-Filtern vermutlich bereits unmittelbar nach dem Upload an eine Mehrzahl Dritter abgeflossen. Es ist nicht feststellbar, welche VirusTotal-Kunden ein hochgeladenes Dokument im Zugriff hatten.

Fragen an IT-Sicherheitsverantwortliche

- Sind Ihre Mitarbeiter, insbesondere IT-Mitarbeiter und Administratoren, bezüglich der Gefahren des Vertraulichkeitsverlustes bei einem Datei-Upload auf Online-Dienste wie VirusTotal sensibilisiert?
- Ist der Upload von Dateien auf Online-Dienste zur Malwareprüfung in Ihrer Institution grundsätzlich untersagt und dies kommuniziert? Sind den Mitarbeitern Alternativen bekannt, z.B. die Suche nach Datei-Hashwerten?
- Wurden in Ihrer Institution Automatismen zur Prüfung auf Online-Diensten eingerichtet? Beispielsweise ein automatisierter Upload von Dateien aus der E-Mail Quarantäne oder aus Sandboxen?
- Sind auch ihre Dienstleister und nachgeordnete Behörden sensibilisiert, denen Sie ggf. BSI-Warnmeldungen weiterleiten?
- Sollten in Einzelfällen doch Prüfungen stattfinden: Wird sichergestellt, dass die Dateien insbesondere keine dem Geheimschutz unterliegenden Inhalte, keine personenbezogenen Daten enthalten und auch keine TLP-Markierung höher als TLP:WHITE haben?

Links

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.