Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Smartphones weltweit von Pegasus überwacht

CSW-Nr. 2021-234348-1032, Version 1.0, 27.07.2021

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

Am 18. Juli 2021 veröffentlichte ein internationales Bündnis aus Journalisten die Ergebnisse einer vorangegangenen Recherche: Demnach war es gelungen, auf den Smartphones von Politikern, Pressevertretern, Menschenrechtlern, Geschäftsleuten und deren Familienangehörigen Spuren der Überwachungssoftware Pegasus zu finden. Auslöser für die Untersuchungen war eine Liste mit 50.000 Telefonnummern angeblicher Überwachungsziele, die Amnesty International und dem Verein Forbidden Stories im Vorfeld zugespielt worden war. Diese Liste konnte den Systemen der NSO Group zugeordnet werden. Das israelische Unternehmen bietet international Überwachungslösungen an [Zeit2021].

Pegasus ist gemäß Medienberichten in der Lage, auf Apple- und Android-Devices Gespräche mitzuschneiden, die Verschlüsselung von Chatnachrichten zu umgehen, Kameras zu aktivieren und Standortdaten auszulesen. Umfangreiche forensische Untersuchungen von Amnesty International [AmIn2021] haben ergeben, dass drei Möglichkeiten zur Verfügung stehen, um die Geräte der Zielpersonen zu infizieren [TagS2021]:

1. Per Smishing, bei dem der Empfänger einer SMS-Nachricht dazu verleitet werden soll, auf einen Link zu klicken, über den Pegasus installiert wird,
2. Per präparierter iMessages (iPhone/iPad), bei denen Pegasus ohne aktive Handlung des Nutzers installiert wird („Zero Click“) oder

* 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.

3. Per Verbindungsaufbau zu einem kompromittierten Netzwerk – wahlweise WLAN oder Mobilfunknetz – bei dem der Angreifer entweder einen Router oder IMSI-Catcher bereitstellt.

Für eine erfolgreiche Infektion nutzt Pegasus den Berichten zufolge bislang unbekannte Zero-Day-Exploits.

Bisher gibt es keine Hinweise darauf, dass auch deutsche Ziele von diesen Aktivitäten betroffen waren.

Bewertung

Das Bedrohungspotenzial ist als hoch zu bewerten, zumal auch aktuelle Versionen von iOS und Android immer noch als verwundbar gelten.

Weiterhin ist davon auszugehen, dass die NSO Group ständig nach neuen Exploits für unterschiedliche Plattformen sucht, sodass selbst bei einer etwaigen zukünftigen Behebung der derzeit genutzten Schwachstellen eine weitere Bedrohung durch Pegasus nicht ausgeschlossen werden kann. Die Berichte, insbesondere der technische Bericht von Amnesty International, lassen darauf schließen, dass sich die Malware-Architektur, die operativen Prozesse und das Tooling zur Verwaltung von Zielen stark auf die Verfügbarkeit von Zero-Day-Exploits ohne Benutzerinteraktion abstützen. Es ist davon auszugehen, dass durch Sicherheitsupdates mitigierte Schwachstellen schnell durch Exploits für andere, neue Schwachstellen ersetzt werden können.

Die Bedrohung durch Pegasus für deutsche Ziele ist demnach nicht durch technische Eigenschaften begrenzt, sondern durch die strategischen Interessen (und davon abgeleitet die Zielauswahl) der Pegasus-nutzenden Kunden.

Bei allen Überlegungen ist jedoch zu beachten, dass es sich beim beschriebenen Sachverhalt den Medienberichten zufolge um dedizierte Angriffe auf einzelne Ziele handelt – nicht um eine auf Massenverbreitung abzielende Kampagne. Infektionen beschränken sich nach aktuellem Kenntnisstand somit auf ausgewählte Personenkreise und Branchen.

Maßnahmen

Aufgrund der Professionalität der Angreifer ist die zielführende **Umsetzung präventiver Schutzmaßnahmen sehr schwierig**.

Organisationen können in Erwägung ziehen, die zur Kompromittierung genutzten Apps und Dienste – Anwendungen zum Öffnen von SMS im Allgemeinen sowie iMessage und Facetime bei Apple-Geräten– in ihrer Nutzung einzuschränken. Eine Deaktivierung kann am Gerät selbst bzw. bestenfalls zentral über ein Mobile Device Management-System vorgenommen werden.

Während die Nutzung von WLAN (Angriffsvektor Nr. 3) ebenfalls noch eingeschränkt werden kann, ist spätestens bei IMSI-Catchern kaum ein praktikabler Schutz möglich. Zwar existieren verschiedene Apps, mit denen derartige Funkzellen erkannt werden sollen, ob diese Apps jedoch auch bei den hier beschriebenen, fortschrittlichen Angriffstechniken helfen, ist unklar.

IT-Verantwortlichen wird daher empfohlen, vor der Umsetzung präventiver Maßnahmen eine Risikoabschätzung durchzuführen. Hierbei sollte neben der eigenen (ggf. nur geringen) Exposition [BSI2021] auch in Betracht gezogen werden, dass sich aus dem Wechsel auf alternative Kommunikationskanäle ggf. neue Bedrohungsszenarien ergeben – bspw. durch unzureichend verschlüsselte, alternative Messenger oder E-Mails. Aufgrund der Professionalität des Angriffswerkzeugs ist außerdem zu vermuten, dass avisierte Ziele kurzfristig über andere Wege infiziert werden können.

Als reaktive Maßnahme empfiehlt sich die Verwendung des von Amnesty International bereitgestellten Mobile Verification Toolkits. Mit dieser Anwendung können Endgeräte auf eine Infektion mit Pegasus untersucht werden [MVT2021]. Die Menschenrechtsorganisation weist jedoch gleichzeitig darauf hin, dass Spuren auf Android-Smartphones in diesem Kontext schwieriger zu finden sind, als auf iPhones/iPads.

Sofern Sie Spuren einer Infektion entdecken, bitten wir Sie um Kontaktaufnahme unter certbund@bsi.bund.de .

Links

[Zeit2021] Cyberangriff auf die Demokratie:
https://www.zeit.de/politik/ausland/2021-07/spionage-software-pegasus-cyberwaffe-ueberwachung-menschenrechte-enthuellung

[AmIn2021] Forensic Methodology Report: How to catch NSO Group's Pegasus:
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[TagS2021] Wie "Pegasus" aufs Handy kommt:
https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-101.html

[BSI2021] Cyber-Sicherheits-Exposition:
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_013.pdf

[MVT2021] MVT – Mobile Verification Toolkit:
https://github.com/mvt-project/mvt

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.