Black Hat Asia 2019

Baldige Altlasten

Philipp Beck

Auf der Black Hat Asia 2019 reüssierte der Begriff „Asbest der IT“ – gemeint war das Internet of Things.

Als Ableger der wohl bekanntesten IT-Security-Konferenz aus Las Vegas hat sich die Black Hat Asia mit ihrer zehnten Ausgabe mittlerweile als Anlaufstelle für die Community etabliert. Ende März lockte sie dieses Jahr Referenten, Zuhörer, Hersteller und Entwickler aus 83 Ländern nach Singapur.

Mehrtägige Schulungsangebote, eine Herstellermesse und das sogenannten Arsenal, bei dem viele kostenfreie Tools der Öffentlichkeit vorgestellt wurden, begleiteten die Vorträge. Beispielsweise präsentierte AttackForge sein webbasiertes Kollaborations- und Trackingtool für Penetrationstests. Mit der ebenfalls gezeigten Cloud Security Suite lassen sich Audits für AWS-, GCP- und Azure-Umgebungen automatisieren, CQTools wiederum fasst 39 Werkzeuge für professionelles Red Teaming zusammen. Eines der Werkzeuge kann unter anderem sämtliche in Windows gespeicherten Kennwörter auslesen – in bestimmten Szenarien sogar die des Passwortmanagers KeePass.

In der Keynote sprach Security-Experte Mikko Hypponen über das Internet als Kriegsschauplatz und von ihm beobachtete Wettrüsten, wie es die Welt zuletzt bei Atomwaffen erlebte. Ein Unterschied sei jedoch, dass frühere Muskelspiele zur Abschreckung nun in den Hintergrund gerieten. Der neue Fokus läge auf einer verdeckten und abstreitbaren Durchführung schädlicher Handlungen. Gerade dies mache die neuen Angriffe so unberechenbar wie gefährlich. Derzeit beginne diese Entwicklung erst – sie begleitet uns womöglich die nächsten Jahrzehnte, ergänzt durch immer neue Felder wie autonome Kampfmaschinen, DNA-Manipulation, Nano-Bots und künstliche Intelligenz.

Gefahr im und durchs IoT

Derzeit sieht Hypponen jedoch in erster Linie die Bereiche IoT und vernetzte Industrieanlagen gefährdet und fragt sich, ob wir dabei sind, das Internet der Dinge zum Asbest der IT werden zu lassen. Während es beim Schutz vor Kriminellen häufig reiche, nicht das leichteste Opfer zu sein, seien staatliche Angriffe hingegen persistent (im Sinne von APT) gegenüber einem einmal ausgewählten Ziel. Und spätestens in einem solchen Szenario sei es utopisch, zu glauben, man könne sämtliche Angriffe abwehren – das Fehlen einer umfassenden Sicht bezüglich erfolgreicher Angriffe auf die eigene Infrastruktur sei daher für viele Organisationen derzeit eine offene Flanke ihrer Verteidigungsstrategie, die sie dringend schließen müssten.

Passend zu den Warnungen Hypponens stellte Security-Forscher Tan Kean Siong im Anschluss seine Analysen zu IoT-Botnetzen vor. Über seinen per Raspberry Pi betriebenen Glutton Honeypot stieß er auf einen Nachfolger der Mirai-Malware, fand in den Logs die Adressen der C&C-Server und konnte dort Gigabyte-weise Quellcode unterschiedlicher Versionen herunterladen sowie analysieren. So beobachtete er Grabenkämpfe der Kriminellen im Hintergrund: Malware löschte Malware auf bereits infizierten Geräten, änderte Passwörter und hackte Backend-Server. Per Instagram und YouTube tauschten sich die Botnet-Betreiber derweil gegenseitig über aktuelle Konferenzbeiträge aus und prahlten mit feindlichen Übernahmen, Monatseinkommen und DoS-Schlagkraft.

Weitere Einblicke in die Hintergründe krimineller Machenschaften konnte Sicherheitsforscher Min-Chang Jang im Bereich Voice Phishing geben. Sein Team analysierte einen neuen Angriff: Kriminelle verleiten ihre Opfer zum Installieren einer Android-Malware, die von da an sämtliche Anrufe an Hotline-Nummern lokaler Banken im Hintergrund auf Telefonnummern der Angreifer umleitet. Der Nutzer bekommt hiervon nichts mit und der Angreifer hat hohe Erfolgschancen, wenn er während dieser Phishing-Telefonate nach Zugangsdaten und TANs fragt.

Baufahrzeuge aus der Ferne übernehmen

Threat-Researcher Philippe Lin und Akira Urano stellten ihre Angriffe auf industrielle Funkfernbedienungen vor, darunter solche für Bau- und Logistikkräne. Bei allen sieben untersuchten Systemen waren sie in der Lage, mit Software-defined Radio Tools wie HackRF und BladeRF eigene Befehle einzuspielen. Mit RFQuack entwickelten sie zudem ein Werkzeug, mit dem sie Zielsysteme auch per Internet über einen Python-Client und einen MQTT-Server steuern können, sobald ein Arduino-basierter Sender mit Mobilfunkanbindung platziert wurde.

Auch die klassische IT wurde auf der Black Hat Asia nicht verschont. Claudio Canella und Moritz Lipp von der Universität Graz stellten sechs neue Varianten der Spectre- und Meltdown-Angriffe vor. Eine Meltdown-Variante betrifft erstmals auch AMD-Prozessoren; zudem gelang es ihnen, aktuelle Patches gegen die bekannten Varianten zu umgehen. Ein Team um Xianbo Wang entdeckte mehrere Redirect-Schwachstellen bei Implementierungen des Single-Sign-on-Frameworks OAuth 2.0 in Kombination mit gängigen Browsern und mobilen Apps. Beispielsweise würde ein Identity-Provider für einen ihm bekannten Serviceprovider good.com Redirect-URLs, die mit einer Ziffer beginnen, wie bei 3vil.com://good.com, als gültig akzeptieren. Bei einem Benutzer mit einem veralteten Safari-Browser würde jedoch die Domäne 3vil.com aufgerufen und das an die URL angehängte Zugangstoken somit in die Hände von dessen Betreibers fallen. (fo@ix.de)