CanSecWest 2019

Eingeheimst

Hagen Molzer

Wer einen Tesla haben will, muss ihn hacken – das galt zumindest auf der diesjährigen CanSecWest und ihrem traditionellen Wettbewerb Pwn2Own.

In der zweiten Märzhälfte lud nunmehr zum neunzehnten Mal die CanSecWest nach Vancouver ein. Viel Aufmerksamkeit zieht jedes Jahr der Pwn2Own-Wettbewerb auf sich. Bei ihm treten Hacker in unterschiedlichen Kategorien gegeneinander an, zum Beispiel 2019 erstmals im Bereich Automotive. Die Gewinner erhalten das gehackte Objekt als Preis; das Team Fluoroacetate, bestehend aus Amat Cama und Richard Zhu, heimsten so ein Tesla Model 3 ein – und ein Preisgeld in Höhe von 35 000 US-Dollar. Sie konnten eine Nachricht auf dem Display des Elektroautos anzeigen, indem sie den Renderer des Browsers im Infotainmentsystem durch einen JIT-Bug (Just-in-time-Kompilierung) angriffen.

Weniger schlagzeilenträchtig sind hingegen die Schulungen, Dojos genannt, die die Security-Konferenz einleiten. Teilnehmer konnten sich dieses Jahr unter anderem in den Bereichen Web Pentesting, Windows Kernel Exploitation und PowerShell aus Sicht von Angreifern und Verteidigern weiterbilden.

Modulare Infrastruktur für Red Teams

Die Vorträge nahmen Hard- und Software aus Sicht der IT-Sicherheit unter die Lupe und wurden innerhalb eines Tracks an den drei Tagen gehalten. Außerdem thematisierten sie aktuelle Themen wie Desinformationskampagnen im Internet und Gegenmaßnahmen.

Sicherheitsforscher Topher Timzen und Michael Leibowith schlugen in ihrem Vortrag Attack Infrastructure for the Modern Red Team ein Design einer professionellen, einfach zu verwaltenden und für parallel stattfindende Einsätze leicht zu vervielfältigenden Infrastruktur vor. Weitere Anforderungen sind, dass die Umgebung modular, leicht anpassbar und gegen Angriffe geschützt ist.

Nachdem sie zunächst den Begriff „Red Teaming“ als „mehr als ein Pentest und das Ziel, einfach Domain-Admin zu werden“ weiter definierten, gingen sie genauer auf ihre Vorstellung einer effizienten Infrastruktur ein: Ihr Design sieht verschiedene Zonen und fest definierte Kommunikationswege über zentrale Proxyserver vor, um die Angriffsfläche auf die Umgebung selbst zu minimieren. Hinzu kommen Konfigurationen zum Verhindern typischer OPSEC-Fehler (Operations Security) des Pentesters selbst, die den Blue-Teams helfen könnten.

Ein weiteres Feature ist das Vorbereiten und Bereithalten mehrerer unauffälliger Domänen, die nicht erst „ein paar Tage alt sind“, sowie ein ausgeklügeltes System zum Terminieren der TLS-Verbindungen des Command-and-Control-Verkehrs aus dem Netz des Opfers. Das alles soll es den Blue-Teams des Kunden schwerer machen, laufende Kampagnen zu erkennen und Gegenmaßnahmen einzuleiten.

Informationen von Windows Hello

Um einfach neue Instanzen der Umgebung für weitere Angriffskampagnen oder Projekte erstellen zu können, empfehlen die Forscher Vagrant und Puppet sowie Git zum Verwalten der Konfigurationen. Zum Visualisieren der Informationen schlagen sie Natlas vor. Kibana und Elastic sammeln die Logdateien und bereiten sie auf. Herzstück der Umgebung sind verschiedene Angriffswerkzeuge wie Cobalt Strike, Metasploit oder Empire, integriert in einer Kali-Installation. Letztere heißt hier Homebase und ist die eigentliche Arbeitsoberfläche für den Pentester.

Im Rahmen ihres Vortrags „Dive into Windows Hello: Is it really more secure than a Password?“ zeigten Hyoung-Kee Choi und Ejin Kim in einer Live-Demo, wie sie die für Windows Hello relevanten Informationen aus einem System extrahieren, auf einem anderen Computer importieren und dort verwenden können. Die sechsstellige PIN, die das Schlüsselmaterial freigibt, lässt sich mit einer durchschnittlichen Notebook-CPU in kurzer Zeit durch einen Brute-Force-Angriff ermitteln.

Einzige Voraussetzung: Der TPM-Schutz ist nicht aktiviert. Geplant ist, dass der Angriff künftig auch bei Hello for Business oder beim Einsatz des TPM funktionieren.

„Memsad: Why Clearing Secrets is Hard“ erklärte, warum Programme immer wieder Schlüssel oder andere Geheimnisse im Arbeitsspeicher zurücklassen, obwohl Entwickler das eigentlich im Programmcode verhindern. Des Rätsels Lösung sind die Optimierungen des Compilers, die die zum Löschen der sensiblen Informationen vorhandenen Befehle entfernen – für den Programmablauf sind sie schließlich nicht nötig. Für Programmierer ist der Vorgang jedoch nicht transparent.

Zwischenzeile

Technisch vergleichbar tief ging der Vortrag „PAC-Man and Ghosts: A practice and breakthrough of Pointer Authentication on iOS“ auf die Technik der Pointer Authentication in ARM Version 8.3 ein. Um das Ausnutzen sogenannter Memory-Corruption-Schwachstellen zu erschweren, versieht das System im Arbeitsspeicher vorgehaltene (Sprung-)Zeiger mit Signaturen. Ohne Kenntnis des dafür verwendeten Schlüssels ist es für einen Angreifer schwierig, gültige Sprungadressen zu erzeugen. (fo@ix.de)

Quelle: Tesla

Überlistet: Das Infotainmentsystem des Model 3 konnten zwei Hacker auf der diesjährigen CanSecWest austricksen – womit sie den Tesla gewannen.