| 17.06.2025

heise security PRO

Jürgen Schmidt
Leiter heise security
ju@heisec.de

Lieber Leser,

um der grassierenden Infostealer-Plage etwas entgegenzusetzen, kündigte Google im Juli 2024 App-Bound Encryption (ABE) an. Infostealer sammeln routinemäßig alle in Chrome – und vielen anderen Browsern – gespeicherten Passwörter, Session-Cookies, Zahlungsdaten und so weiter ein. Die verschlüsselt Chrome zwar, aber jeder Prozess mit den Rechten des angemeldeten Benutzers kann sie etwa unter Windows mit einem Aufruf des Data Protection Application Programming Interface entschlüsseln. ABE sollte das auf legitime Chrome-Prozesse beschränken; der Infostealer mit Benutzerrechten hätte keinen Zugriff mehr.

Natürlich war unmittelbar klar, wie sich das umgehen ließe: Entweder mit Adminrechten oder via Process Injection. Das ist eine etablierte Angriffstechnik, bei der der Infostealer Code in einen legitimen Chrome-Prozess einschleust. Jeder Malware-Coder, der etwas auf sich hält, hat das drauf und kann damit an ABE vorbei alle gespeicherten Passwörter und andere geschützte Credentials auslesen. Es dauerte folglich nicht einmal zwei Monate und so gut wie alle Hersteller von Infostealern verkündeten Erfolg: Lumma, Vidar & Co oder genauer gesagt deren kriminelle Kunden konnten bereits ab September wieder auf alles zugreifen – trotz ABE.

RIP Chrome ABE – Analyse und PoC

Jetzt hat sich ein Sicherheitsforscher der Sache angenommen. Er demonstriert mit einem quelloffenen Tool, wie man via Process Injection alle Passwörter, Cookies und Zahlungsdaten aus Chromium-basierten Browsern wie Chrome, Edge und Brave auslesen kann – ganz ohne Adminrechte. Nebenbei dokumentiert er die Funktionsweise und Interfaces der App-Bound Encryption.

ABE ist keine Mitigation, sondern demonstriert lediglich Hilflosigkeit. Dem setzt Chrome App-Bound Encryption Decryption jetzt das verdiente Ende.

Hardware bound Credentials FTW!
Gegen Passwort-Diebstahl schützt Multi-Faktor-Authentifizierung, am besten in der Variante mit Hardware-bound FIDO2-Tokens. Doch das umgehen Kriminelle, indem sie Session- oder Refresh-Tokens abgreifen und missbrauchen. Auch hier ist klar, wie Schutz vor Infostealern aussehen müsste, der den Kriminellen ernst zu nehmende Hürden in den Weg stellt. Google selbst hat dazu Device Bound Session Credentials (DBSC) entworfen und teilweise auch schon umgesetzt. Sie koppeln die Credentials kryptografisch an ein Gerät; das funktioniert mit diebstahlsicher im TPM abgelegten Geheimnissen und asymmetrischer Kryptografie.

Der Infostealer kann das Session-Cookie zwar immer noch stehlen, es wird aber auf seinem Gerät nicht funktionieren. Das Problem dabei ist, dass man DBSC anders als ABE nicht allein im Browser umsetzen kann, sondern die Web-Dienste da mithelfen müssen. Denn die müssen sich regelmäßig die Gültigkeit der DBSC-Cookies bestätigen lassen. Hier beschreiben zwei Google-Devs, wie man das sinnvoll umsetzen kann. Bis das flächendeckend ausgerollt ist, wird es allerdings leider noch etwas dauern.

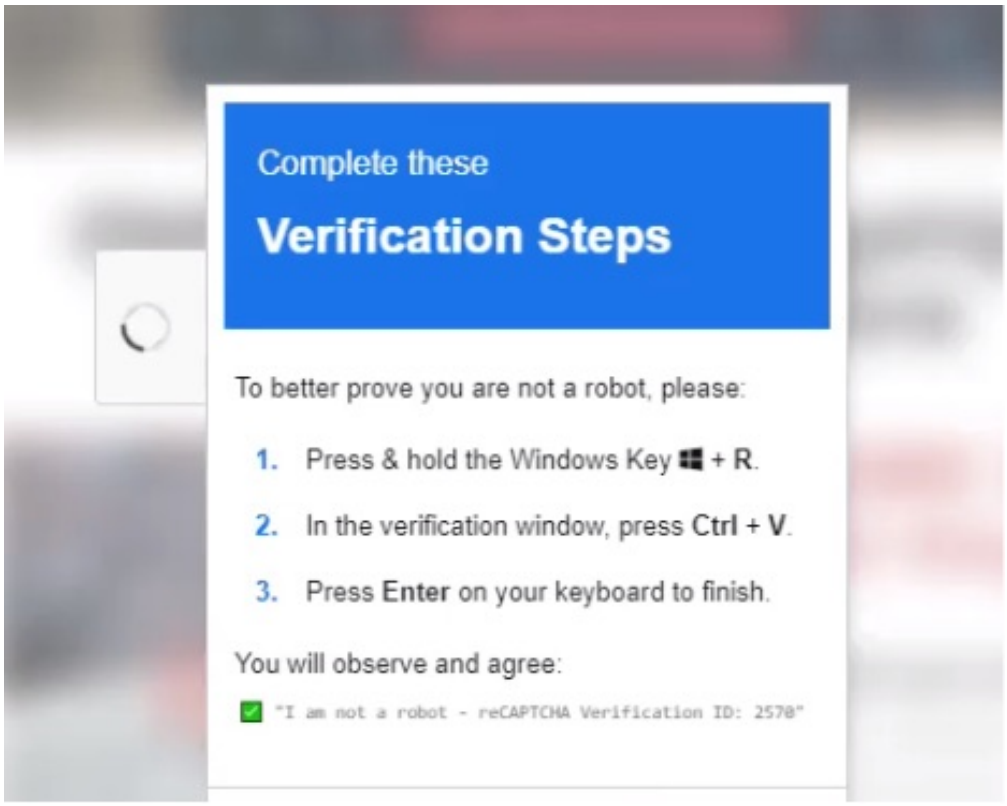
Chrome mit lokaler KI gegen Betrugsversuche

Google hat ein neues Einsatzszenario für KI ausgemacht: betrügerische Web-Seiten erkennen und in Chrome blockieren, bevor sie angezeigt werden. Das LLM Gemini Nano soll bereits ab Chrome 137 den etablierten Schutz durch das Safe Browsing API verbessern. Safe Browsing sperrt den Zugriff auf bekannte Scam-Seiten. Doch diese seien mittlerweile so extrem kurzlebig, dass Crawler sie kaum mehr zu Gesicht bekämen. Bevor die URLs in Googles Sperr-Datenbanken landen, ist die Seite längst woanders.

Ich war zunächst angenehm überrascht, dass Google das ganz freiwillig "on-device", also lokal beim Anwender macht. Sollte der Konzern zu seinen datenschutzfreundlicheren, "Don't be evil"-Wurzeln zurückkehren? Doch nein, die Begründung zu "But why on-device?" belehrte mich sofort eines Besseren: Das geht lokal einfach schneller. Außerdem erlaube es der On-Device-Ansatz, "die Bedrohungen genau so zu sehen wie der Anwender". Big Brother Google schaut mir also beim Surfen ganz selbstverständlich über die Schulter. Immerhin betrifft das im Idealfall nur vermutlich betrügerische Web-Sites – oder? ODER?

Der ClickFix-Trick

Noch einmal zur Gefahr durch Infostealer: Nach Qualys, Netskope, Cybereason, Kaspersky und nicht zuletzt diesem Newsletter warnt jetzt auch Sophos davor, dass der Infostealer Lumma Captchas vorgaukelt, um sich auf dem System seiner Opfer zu installieren. Letztlich läuft es darauf hinaus, dass das Lumma-Captcha sein Opfer aufgefordert, eine Shell zu starten (WIN-R) und dort Code einzufügen (CTRL-V). Das Clipboard hatte die Web-Seite selbst mit den passenden Anweisungen für Download und Start des Lumma-Infostealers befüllt; das Opfer muss diese dann nur noch mit "Enter" abschicken.



Quelle: Cybereason

Ich erwähne das hier aus zwei Gründen erneut: Lumma ist aktuell einer der beliebtesten Infostealer der Cybercrime-Szene. Sprich: Die Gefahr ist akut. Und die Kombination WIN-R/CTRL-V/Enter ist ein weitverbreiteter, nicht auf Lumma beschränkter Trick. Microsoft bezeichnet das – warum auch immer – als ClickFix. Auf diesen Security-Fallstrick solltest du deine Kollegen unbedingt vorbereiten. Denen ist nämlich nicht zwangsläufig bewusst, dass sie sich damit ins Knie schießen.

Die Lockbit-Leaks

Wie bereits im letzten Newsletter erwähnt, wurde die gerade neu aufgebaute Infrastruktur des ehemaligen Ransomware-Primus Lockbit von Unbekannten gehackt. Im Zuge dessen tauchte ein großes Datenpaket auf, das unter anderem Chats, interne Abläufe und auch Verhandlungen mit Opfern dokumentiert. Das ist spannendes Material für Forscher und Strafverfolger; für Verteidiger habe ich da bisher jedoch wenig Neues und Erhellendes entdeckt, das nicht etwa über die Conti-Leaks bereits bekannt ist. Qualys weist in seiner Analyse aber auf einen interessanten Aspekt hin: Offenbar bevorzugte Lockbit die Bezahlung über Monero statt Bitcoin und gab dafür sogar Rabatte von bis zu 20 Prozent.

Monero hat sich bereits seit einiger Zeit in den Untergrund-Marktplätzen als die Währung der Wahl etabliert, weil sich damit anders als bei Bitcoin die

Transaktionen nicht verfolgen lassen. Auch Qualys begründet die Bevorzugung von Monero für Ransomware-Zahlungen mit dem "datenschutzfreundlichen Design" der Krypto-Währung. Ich würde da noch einen Schritt weitergehen: Lockbit spart bei Monero das aufwendige und teure Waschen der Einnahmen über Mixer und gibt einen Teil der Einsparungen an seine "Kunden" weiter. Das ist Kapitalismus und Teil der Industrialisierung von Cybercrime.

Die "SSO-Steuer" auf SaaS-Produkte

Eine zentrale Anmeldung für alle Dienste, die in deinem Unternehmen genutzt werden – das ist ein wichtiges Security-Feature. Schließlich kannst du durch Single Sign-On flächendeckend MFA einführen, musst erheblich weniger Zugangsdaten und -tokens verwalten, das On- und Offboarding wird einfacher und im Fall eines Breaches sind alle Zugänge in Minuten gesperrt.

Viele SaaS-Anbieter lassen sich diese Funktion aber teuer bezahlen. Sie bieten dann die Anbindung an externe SSO, etwa per OAuth, erst in der teuren "Enterprise"-Variante ihrer Produkte und schlagen teilweise mehrere hundert Prozent auf den Monatspreis. So etwa Github: Möchtest du deren Code- und Projektverwaltung mit SAML-SSO nutzen, zahlst du statt vier US-Dollar pro Monat derer 21, also einen Aufschlag um über 400 Prozent. Weitere Beispiele gibt es online auf der Web-Seite der SSO Wall of Shame.

Warum SSO ein "Enterprise Feature" sein sollte, ist mir schleierhaft – schließlich ergibt es auch für kleine Unternehmen sehr viel Sinn – ja, selbst für Privatleute, die nicht mit X Zugangsdaten jonglieren möchten.

Android bekommt innovativen Lockdown-Modus

Google bestätigt jetzt offiziell, dass es in Android 16 einen "Advanced Protection"-Schalter geben soll, der die Balance zwischen Security und Komfort ein Stück weiter Richtung Sicherheit verschiebt. Ich hielt das bislang nur für den längst überfälligen Schritt, mit dem Google auf Apples Lockdown-Mode für iOS reagiert. Doch die Google-Ingenieure bringen auch eine wichtige Neuerung, die Apple hoffentlich unter Druck setzen wird: Intrusion Logging. Das soll dafür sorgen, dass ein angegriffener Benutzer – oder von ihm beauftragte Spezialisten – nach einem vermuteten Vorfall herausfinden können, was da genau passiert ist.

Dabei soll das Gerät manipulationssichere Security-Logs ende-zu-ende-verschlüsselt in der Cloud sichern, die damit nur für den Anwender zugänglich

sind. Natürlich wird das auch Begehrlichkeiten bei Strafverfolgern wecken, aber wir benötigen dringend mehr Informationen, um mit vermuteten Angriffen sinnvoll umgehen zu können. Und Apple ist da ein extremes Negativ-Vorbild. Apple liebt Black Boxes; der Nutzer soll blind darauf vertrauen, dass Apple schon das Richtige (™) tut. Inspectability, also die Möglichkeit in die Geräte hineinzuschauen, um zu verstehen, was da wie passiert oder auch schiefgeht, ist ihnen ein Graus. Google setzt da einen wichtigen Impuls hin zu mehr Transparenz.

Mit LoLbins am EDR vorbei

Ein sich aktuell abzeichnender Trend bei kriminellen Aktivitäten ist der gezielte Einsatz von bereits vorhandenen oder zumindest legitimen Tools – das "Living of the Land", kurz LoL und die danach benannten LoLBins. Da muss dann die Endpoint Protection anhand der Aufruf-Parameter entscheiden, ob das jetzt der legitime Admin ist, der gerade mit certutil.exe hantiert, oder ein Eindringling, der es missbraucht, um etwa zusätzliches Werkzeug nachzuladen. Dir ist natürlich längst klar, wohin das führt: zum altbekannten Hase/Igel-Rennen bei der Erkennung von bösartigen Aktivitäten.

Wietze Beukema hat sich des Problems Command-Line Obfuscation angenommen und dokumentiert Shell-unabhängige Methoden, wie man Ungenauigkeiten beim Parsing der Argumente ausnutzen kann, um AV und EDR zu umgehen. Sein Open-Source-Tool ArgFuscator liefert obfuszierte Kommandozeilenbefehle, die Defender & Co austricksen, frei Haus. Und wie üblich sehen die Detection-Tools da nicht sonderlich gut aus.

Unser PRO-Talk zu EDR & Co

Apropos Sinn & Unsinn von Antiviren-Software und deren Nachfolger EDR, XDR und wie sie alle heißen. Hättest du nicht mal Lust, dich darüber mit jemandem zu unterhalten, der diesen Schutzprogrammen systematisch auf den Zahn gefühlt hat? Andreas Marx, Mitgründer und Ex-Geschäftsführer des renommierten Testinstituts AV-Test, hat das über viele Jahre hinweg gemacht und kennt deshalb die Stärken und Schwächen einzelner Produkte und auch der jeweiligen Gattungen wie kaum ein anderer. Und nächsten Dienstag ist er zu Gast bei unserem PRO-Talk: "Was du schon immer über Malware-Schutz wissen wolltest (aber nicht zu fragen wagtest)". Meld dich am besten gleich hier an und bring deine Fragen mit. Keine Scheu: Für das Event gilt wie immer die Chatham House Rule und es wird nicht aufgezeichnet.

Das war's für heute, bis hoffentlich Dienstag beim PRO-Talk. Schönen Tag noch, ju.

Impressum

Heise Medien GmbH & Co. KG, Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: +49 [0]511 5352-0, E-Mail: webmaster@heise.de
Registergericht Hannover HRA 26709, Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH, Registergericht Hannover HRB 60405
Geschäftsführer: Ansgar Heise, Beate Gerold

Alle Preise inkl. MwSt.

.