Die Methode Netwalker

Sophos-Experten analysieren Technik und Dramaturgie hinter der Erpressungssoftware, die jüngst u.a. das österreichische Weiz traf.
Der „Werkzeugkasten" der Hacker enthält dabei auch Programme, die zunächst einmal nicht mit Cyberkriminalität verbunden werden…

Tu Schlechtes und rede darüber...diese Abwandlung eines allgemein bekannten Sprichworts haben die Kriminellen hinter der Ransomware Netwalker zuletzt in Österreich verwendet: Wenige Tage ist es her, dass die Cyber-Gangster höchstselbst über Twitter bekannt gaben, die Computer der Stadtverwaltung von Weiz in der Oststeiermark mit der Ransomware infiziert zu haben. Als Beweis für ihre brisante Beute machten sie vertrauliche Daten etwa zu Aktenvermerken, Flurbereinigungsverfahren, baupolizeilichen Prüfungen oder Bauanträgen im Netz öffentlich.

Einblicke in den Werkzeugkasten der Cybergangster
Die Cybergangster hinter Netwalker haben bereits diverse Ziele in den USA, Australien und Westeuropa angegriffen. Gabor Szappanos und Andrew Brandt, führende Researcher bei den SophosLabs, haben Netwalker bereits länger im Visier und sind bei der aktuellen Analyse auf interessante Details gestoßen, die Einblicke in die Arbeit der Netwalker-Schöpfer jenseits der reinen Ransomware-Attacke zulassen. Bei der Untersuchung einer Malware-Kampagne mit dieser Erpressungssoftware stießen sie auf eine Reihe von aufschlussreichen Dateien, die bei den Angriffen als Werkzeuge verwendet und von den Kriminellen zurückgelassen wurden. Sowohl der Fundort der Schadsoftware als auch die verwendeten Dateien enthüllen dabei interessante Details über die Methoden, mit denen die Angreifer Netzwerke kompromittieren und die Malware an Arbeitsplatzrechner verteilen. Zu den Angriffswerkzeugen gehörten dabei unter anderem auch legitime, öffentlich verfügbare Software (wie TeamViewer), Dateien, die aus öffentlichen Code-Repositories (wie Github) abgekupfert wurden und Skripte, die von den Angreifern augenscheinlich selbst erstellt wurden.

Deutlich wird neben den Angriffsorchestrierungen auch, dass die Kriminellen es nicht auf private Opfer, sondern auf Unternehmen und größere Organisationen abgesehen haben. So wurden beispielsweise Programme zur Erfassung von Domänenadministrator-Anmeldeinformationen aus einem Unternehmensnetzwerk zurückgelassen, kombiniert mit Orchestrierungswerkzeugen, die Softwareverteilung über einen Domänencontroller einsetzen, wie sie in Unternehmensnetzwerken üblich, aber bei Privatanwendern selten sind.

In ihrem Blog-Artikel geben die Sophos-Forscher einen detaillierten Überblick über ihre Erkenntnisse und gewähren Einsicht in das typische Verhalten dieses Bedrohungsakteurs.
https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de