Spionagegruppe nimmt militärische Einrichtungen und diplomatische Vertretungen ins Visier - ESET-Forscher analysieren neueste Kampagne der InvisiMole-Gruppe

Bei der aktuellen Malware-Kampagne der InvisiMole-Gruppe deckten ESET-Forscher ihre neuesten Werkzeuge sowie bisher unbekannte Details über ihre Arbeitsweise auf. Gezielte Angriffe auf hochkarätige Organisationen im militärischen Sektor und diplomatische Vertretungen in Osteuropa charakterisieren diese neue Aktion der Cyberspione. Die Untersuchungsergebnisse stammen aus einer tiefgehenden Analyse der ESET-Experten in Zusammenarbeit mit den betroffenen Organisationen.
Die Auswertung der ESET-Telemetriedaten zeigt, dass die Attacken von Ende 2019 bis zur Veröffentlichung des Forschungsberichts andauerten. Im Rahmen der derzeit veranstalteten ESET Virtual World stellen die Experten des europäischen IT-Sicherheitsherstellers ihre Ergebnisse erstmalig der Öffentlichkeit vor. Der vollständige Bericht und das Whitepaper sind ab sofort auf Welivesecurity online verfügbar.

"Bereits in der Vergangenheit machte die InvisiMole-Gruppe mit hochentwickelten Backdoors auf sich aufmerksam. Es fehlte uns aber der Einblick in die Hintergründe - wie die Schadprogramme verteilt, wie sie verbreitet werden und wie sie auf die Systeme gelangen", erklärt ESET-Forscherin Zuzana Hromcová, die InvisiMole eingehend untersuchte. "Mit diesem dazugewonnenen Wissen aus dieser aktuellen Analyse werden wir die bösartigen Aktivitäten der Gruppe zukünftig noch genauer verfolgen können."

ESET erhält tiefe Einblicke in die Arbeitsweise von InvisiMole

Dank der Zusammenarbeit mit den betroffenen Organisationen hatten die ESET-Forscher die Möglichkeit, einen genauen Blick auf die Operationen von InvisiMole zu werfen. "In unserer Analyse konnten wir den umfangreichen Werkzeugkasten der Gruppe genauestens unter die Lupe nehmen, der für die Lieferung, die Bewegung im Netzwerk und das Ausführen der Backdoors verwendet wurde", führt Anton Tscherepanow, leitender ESET Malware Researcher im Fall InvisiMole weiter aus.

ESET-Analyse belegt Zusammenarbeit zweier Spionagegruppen

Eines der Hauptergebnisse der Untersuchung betrifft die Zusammenarbeit der InvisiMole-Gruppe mit einer anderen Spionagegruppe namens Gamaredon. Die Forscher fanden heraus, dass die Werkzeuge und Schadprogramme von InvisiMole erst zum Einsatz kommen, nachdem Gamaredon bereits in das Netzwerk des attackierten Ziels eingedrungen ist. Die ESET-Forscher vermuten, dass die Angriffe auf wichtige Ziele von der relativ einfachen Gamaredon-Malware auf die fortgeschrittene InvisiMole-Malware aufgerüstet werden.

Dies hilft der Gruppe, mit ihren Schadprogrammen unentdeckt zu bleiben und ihr Vorgehen besser zu verschleiern. Hierzu nutzt InvisiMole vier verschiedene Ablaufketten, bei denen Schadcode mit legitimen Tools und anfälligen ausführbaren Dateien erstellt wurden. Damit das eigentliche Schadprogramm von den Sicherheitsforschern nicht erkannt wird, verschlüsselt es die Komponenten bei jedem Opfer individuell Darüber hinaus enthält das neue Werkzeugset auch eine neue Funktion namens DNS Tunneling. Dadurch wird die Kommunikation mit dem C&C-Server getarnt.

Über InvisiMole

nvisiMole ist laut Einschätzung der Experten des europäischen IT-Sicherheitsherstellers mindestens seit 2013 aktiv. ESET-Forscher haben über sie schon 2018 im Zusammenhang mit gezielten Spionageaktivitäten in Russland und der Ukraine berichtet.