Threat-Hunter-Analyse: Neue Ransomware-Gruppe mischt die Szene auf

Warlock reiht sich seit Anfang des Jahres mit zahlreichen Attacken, die Ideenreichtum mit klassischen Techniken kombinieren, in der oberen Liga der Ransomware-Bedrohungsszene ein.

Forscher der Sophos Counter Threat Unit™ (CTU) haben eine Bedrohungsgruppe, die sich selbst als Warlock Group bezeichnet, näher unter die Lupe genommen. Die Cyberkriminellen, die von den Forschern als GOLD SALEM verfolgt werden, kompromittieren seit März 2025 Netzwerke und setzen dabei ihre „Warlock-Ransomware“ ein.

Opfer reichen von kleinen kommerziellen Organisationen bis zu multinationalen Konzernen.
Die 60 veröffentlichten Opfer der Gruppe weisen kein bestimmtes Angriffsziel aus. Zu den Opfern von GOLD SALEM zählen kleine kommerzielle oder staatliche Einrichtungen bis hin zu großen multinationalen Konzernen in Nordamerika, Europa und Südamerika. Wie die meisten Ransomware-Gruppen hat GOLD SALEM es trotz der großen Anzahl potenzieller Ziele weitgehend vermieden, Organisationen in China und Russland anzugreifen. Am 8. September veröffentlichte die Gruppe jedoch ungewöhnlicherweise den Namen eines in Russland ansässigen Opfers auf ihrer Leak-Site. Das kommerzielle Unternehmen bietet Ingenieurdienstleistungen und Ausrüstung für die Stromerzeugungsindustrie an. Obwohl die Russische Föderation eine große Anzahl globaler Ransomware-Distributoren beherbergt, ist sie dafür bekannt, Gruppen, die Organisationen in Russland und seinen Nachbarländern angreifen, aggressiv zu verfolgen. Die Auflistung eines russischen Opfers durch GOLD SALEM deutet darauf hin, dass sie Gruppe möglicherweise von außerhalb dieser Gerichtsbarkeit operiert.

GOLD SALEM war bis zu einem Beitrag im RAMP-Underground-Forum im Juni 2025 nicht öffentlich präsent. Darin forderte ein Vertreter der Gruppe Exploits für gängige Unternehmensanwendungen (zum Beispiel Veeam, ESXi, SharePoint) sowie Tools zur Deaktivierung von Endpoint Detection and Response (EDR)-Systemen und anderen Sicherheitsprodukten. In einem nachfolgenden Beitrag wurde um die Zusammenarbeit mit Initial Access Brokern (IABs) bei der Bereitstellung potenzieller Opfer gebeten. Es ist unklar, ob die Gruppe Zugriff für eigene Angriffe suchte, Partner für eine Ransomware-as-a-Service (RaaS)-Operation rekrutierte – oder beides im Sinn hatte.

Kriminelle sind mit Mix aus bekannten Strategien erfolgreich
Ende Juli analysierten CTU-Forscher einen Vorfall, bei dem GOLD SALEM die ToolShell-Exploit-Kette für den Erstzugriff auf SharePoint-Server nutzte. Diese Exploit-Kette verwendete eine Kombination der Schwachstellen (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771) und ermöglicht es dem Angreifer, beliebige Befehle aus der Ferne ausführen und sich die resultierenden Ergebnisse anzeigen lassen. Die heruntergeladene ausführbare Datei war ein Golang-basierter WebSockets-Server, der unabhängig von der Web-Shell weiterhin Zugriff auf den kompromittierten Server ermöglichte. CTU-Forscher beobachteten außerdem, wie die Gruppe eine EDR-Lösung umging, indem es die BYOVD-Technik (Bring Your Own Vulnerable Driver) und einen anfälligen Baidu Antivirus-Treiber (umbenannt in googleApiUtil64.sys) nutzte, um den EDR-Agenten zu beenden. Eine Schwachstelle in diesem Treiber (CVE-2024-51324) ermöglicht die Beendigung beliebiger Prozesse.

Microsofts Profil der Gruppe vermerkt zudem die Ausführung von Mimikatz, „das gezielt auf den Speicher des Local Security Authority Subsystem Service (LSASS) abzielte, um Klartext-Anmeldeinformationen zu extrahieren“. Microsoft beobachtete außerdem die Verwendung von PsExec und Impacket für laterale Bewegungen sowie die Verwendung von Gruppenrichtlinienobjekten (GPO) zur Bereitstellung der Warlock-Nutzlast.

Im August beobachteten CTU-Forscher, wie GOLD SALEM das legitimierte Open-Source-Tool Velociraptor für digitale Forensik und Incident Response (DFIR) missbrauchte, um einen Visual-Studio-Code-Netzwerktunnel innerhalb der kompromittierten Umgebung einzurichten. Einige dieser Vorfälle endeten mit der Bereitstellung der Warlock-Ransomware.

Alle Details zur Analyse sowie dedizierte Threat-Indikatoren gibt es im englischen Blogartikel.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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