Cyberkriminelle nutzen massenhaft virtuelle Maschinen auf legitimen Hosting-Infrastrukturen

Sophos-Forensik zeigt, dass Cyberkriminelle tausende virtuelle Maschinen auf legitimen Hosting-Infrastrukturen missbrauchen, insbesondere in Russland, aber vermehrt aufgrund der leistungsfähigen Infrastruktur auch in den Niederlanden und Deutschland.

Ende 2025 untersuchte die Sophos Counter Threat Unit (CTU) mehrere Ransomware-Vorfälle im Zusammenhang mit WantToCry. In allen analysierten Fällen nutzten die Angreifer virtuelle Maschinen mit automatisch generierten NetBIOS-Hostnamen, die aus Windows-Templates des legitimen Infrastrukturmanagement-Anbieters ISPsystem stammten. Sophos CTU nahm diese Beobachtung zum Anlass, Umfang und Hintergründe des Missbrauchs dieser Infrastruktur näher zu untersuchen und kam zu dem Ergebnis, dass zahlreiche öffentlich erreichbare Systeme mit diesen Hostnamen mit Cybercrime-Aktivitäten in Verbindung standen. Dazu zählten Ransomware-Operationen, der Einsatz von Remote-Access-Trojanern sowie die Verbreitung gängiger Malware. Besonders auffällig waren die Hostnamen WIN-J9D866ESIJ2 und WIN-LIVFRVQFMKO, die nicht nur in WantToCry-Angriffen auftauchten, sondern auch in Kampagnen mit LockBit-, Qilin- und BlackCat-(ALPHV)-Ransomware sowie beim Einsatz des NetSupport RAT.

Wiederkehrende Hostnamen über Jahre hinweg
Auch historische Erkenntnisse unterstreichen die wiederholte Nutzung identischer Hostnamen durch unterschiedliche Akteure. So wurde bereits 2021 ein System mit dem Hostnamen WIN-LIVFRVQFMKO für den Zugang zu internen Chats bekannter Cybercrime-Gruppierungen genutzt. Diese Chats wurden im Rahmen der sogenannten „ContiLeaks“ öffentlich. In den darauffolgenden Jahren tauchte derselbe Hostname unter anderem bei einer Ursnif-Kampagne gegen italienische Organisationen sowie bei der Ausnutzung einer Schwachstelle in FortiClient EMS auf.

Eine Auswertung mit der Suchmaschine Shodan zeigte, dass diese Hostnamen nicht einzelnen Systemen oder Akteuren zugeordnet werden können. Im Dezember 2025 waren mehrere tausend internetexponierte Systeme mit identischen Hostnamen aktiv, die unter anderem RDP-Dienste anboten. Der Großteil dieser Systeme befand sich basierend auf der zugehörigen IP-Adresse in Russland, an Platz 2 und 3 liegen Deutschland und die Niederlande. Die beiden westeuropäischen Länder rangieren vermutlich sehr weit oben, da sie aufgrund ihrer strategisch zentralen Lage, ihrer sehr guten Anbindung über große Internetknotenpunkte (AMS-IX und DE-CIX), ihrer strengen, DSGVO-konformen Datenschutzgesetze und ihrer robusten, nachhaltigen Infrastruktur führende europäische Hosting-Zentren sind und für hohe Geschwindigkeiten und geringe Latenzzeiten stehen.

Auffällige Hosting-Anbieter und staatliche Bezüge
Zwar ist davon auszugehen, dass ein Teil dieser Systeme legitim genutzt wird, doch weitere Daten deuten auf enge Verbindungen zwischen bestimmten Hosting-Anbietern und cyberkriminellen beziehungsweise staatlich unterstützten Aktivitäten hin. Zwei Anbieter – Stark Industries Solutions Ltd und First Server Limited – traten dabei besonders hervor. Gegen Stark Industries Solutions Ltd verhängte der Europäische Rat im Mai 2025 restriktive Maßnahmen wegen der Unterstützung russischer staatlicher und staatsnaher Akteure. First Server Limited wird laut Drittanalysen mit der russischen Desinformationskampagne „Doppelganger“ in Verbindung gebracht.

Technische Ursache: Nicht-randomisierte Windows-Templates
Die Häufung identischer Hostnamen lässt sich technisch erklären: Sie stammen aus weit verbreiteten Windows-Server-Images, die über die Virtualisierungsplattform ISPsystem VMmanager bereitgestellt werden. CTU-Forscher konnten in Tests bestätigen, dass diese Templates Hostnamen und Zertifikate enthalten, die bei der Bereitstellung nicht randomisiert werden. Besonders häufig werden sogenannte KMS-aktivierte Images eingesetzt, die einen zeitlich begrenzten, lizenzfreien Betrieb ermöglichen.

Alle vier am häufigsten verwendeten Hostnamen – sie machen über 95 Prozent der öffentlich erreichbaren ISPsystem-VMs aus – konnten mit kriminellen Aktivitäten in Verbindung gebracht werden. Darüber hinaus fanden die Forscher in Untergrundforen und auf Telegram zahlreiche Hinweise auf Bulletproof-Hosting-Anbieter, die gezielt solche Infrastruktur vermarkten. Besonders häufig wurde der Anbieter MasterRDP (auch bekannt als rdp.monster) genannt, der offenbar eigene, missbrauchstolerante Hosting-Infrastruktur betreibt.

Der ISPsystem VMmanager selbst ist eine legitime und weit verbreitete Virtualisierungsplattform und nicht bösartig. Niedrige Kosten, einfache Bereitstellung und standardisierte Templates machen die Lösung allerdings auch attraktiv für Cyberkriminelle, da die große Zahl legitimer Nutzer als Tarnung für missbräuchliche Aktivitäten dient.

Den kompletten Artikel lesen Sie bitte im Sophos-Blog unter https://www.sophos.com/en-us/blog/malicious-use-of-virtual-machine-infrastructure

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