Kurzzusammenfassung

Snake-Malware

Allgemeines

Das Snake-Implantat gilt als das ausgeklügeltste Cyber-Spionage-Tool, das vom Center 16 des Russischen Föderalen Sicherheitsdienstes (FSB) entwickelt und verwendet wird, um langfristige Geheimdienstsammlungen über sensible Ziele durchzuführen.

Zur Durchführung von Operationen mit diesem Tool hat der FSB ein verdecktes Peer-to-Peer (P2P)-Netzwerk aus zahlreichen weltweit infizierten Computern mit Snake erstellt. Viele Systeme in diesem P2P-Netzwerk dienen als Relaisknoten, die den getarnten Betriebsverkehr zu und von Snake-Implantaten zu den eigentlichen Zielen des FSB routen. Snakes individuelle Kommunikationsprotokolle verwenden Verschlüsselung und Fragmentierung zur Wahrung der Vertraulichkeit und sind darauf ausgelegt, die Erkennung und Erfassung zu erschweren.

Verteilung

Es gab identifizierte Snake-Infrastrukturen in über 50 Ländern auf der ganzen Welt, darunter Nordamerika, Südamerika, Europa, Afrika, Asien und Australien, einschließlich der Vereinigten Staaten und Russland selbst.

Weltweit hat der FSB Snake eingesetzt, um sensible Geheimdienstinformationen von hochpriorisierten Zielen zu sammeln, wie Regierungsnetzwerken, Forschungseinrichtungen und Journalisten.

Dauer bis zur Stilllegung

Der FSB begann Ende 2003 mit der Entwicklung von Snake unter dem Namen „Uroburos“. Damit sprechen wir von einer Laufzeit von fast 20 Jahren.

Attribution

Snake-Operationen werden einer bekannten Einheit innerhalb von Center 16 des FSB zugeschrieben. Diese Einheit betreibt im weiteren Sinne die zahlreichen Elemente des Turla-Toolsets und verfügt über Untergruppen, die in ganz Russland verteilt sind und sich an historischen Signal-Intelligence-Operationen des KGB in der Sowjetunion orientieren.

Smart Data Center GmbH
Südportal 3
22848 Norderstedt

+49 40 741 24 16 0
kontakt@smart-datacenter.de
www.smart-datacenter.de

Was über groß angelegte, zumeist staatlich subventionierte Malware wie Snake bekannt sein sollte, aber vielen nicht klar ist

- Wir sprechen hier von einem großen Entwicklungsteam bzw. mehreren, die zu verschiedenen Teilen dieses Malware-Ökosystems beitragen. Am ehesten entspricht das dem Betrieb eines Unternehmens für Softwareentwicklung mit mehreren Abteilungen. Es handelt sich um ein großes Entwicklungsteam von mindestens 50 - 250, wenn nicht sogar mehr Spezialisten, die an dem „Produkt“ mitwirken.
- Auch wenn Snake verschwinden wird, die Entwickler bzw. die Einheit, die dafür verantwortlich ist, wird es nicht. Das heißt die Entwicklung geht ungebrochen weiter. Der Verlust des Netzwerks ist zwar für den FSB bedauerlich, wird aber schnell durch ein neues System ersetzt werden.
- Noch wichtiger zu wissen ist aber wohl, dass bei so einer Operation immer schon Pläne in der Schublade liegen, was im Falle einer Enttarnung zu tun ist. Wir vermuten, dass ein Ersatzsystem bereits jetzt zur Verfügung steht und in diesem Moment ausgerollt bzw. aktiviert wird.
- Eine weitere Möglichkeit, die berücksichtigt werden muss, ist, dass es Möglichkeiten des „Recyclings“ gibt. Snake wird vielleicht nie ganz verschwinden, sondern in veränderter Form wieder aktiviert werden.
- Insgesamt muss man sich vor Augen halten, dass die Gefahr nicht sinkt, sondern steigen wird. Diese Teams werden sich weiterentwickeln und aus ihren Fehlern lernen. Daraus sollte man schließen, dass die nächste Enttarnung schwieriger wird und wir dementsprechend in Zukunft mehr in Prävention und Gegenmaßnahmen investieren müssen.
- Weiterhin sollte man nicht dem Irrglauben anheimfallen, dass der Mittelstand oder auch kleinere Gemeinden ein uninteressantes Ziel für solche Gruppierungen wären. Das Gegenteil ist der Fall. Jeder übernommene Computer kann Teil eines versteckten Netzwerkes werden, mit dem sensible Daten übermittelt und schlimmer noch einer Verfolgung entzogen werden. Und wenn es der Sache der Gruppierung dienlich ist, wird sie nicht zögern, diese Infrastruktur zu opfern, um sich einer Enttarnung zu entziehen – das wäre dann ein sogenannter Kollateralschaden cybertechnischer Natur.
- Snake ist nur EIN Beispiel und es gibt weitere Staaten, die ihre eigenen Gruppen mit ähnlichen Mitteln haben.

Smart Data Center GmbH
Südportal 3
22848 Norderstedt

+49 40 741 24 16 0
kontakt@smart-datacenter.de
www.smart-datacenter.de

Wie hätte die Smart Data Center GmbH zur Verhinderung beitragen können?

- Virtualisierte Systeme können besser überwacht und gewartet werden.
- Virtualisierte Systeme können regelmäßig KOMPLETT bereinigt werden, was man bei Hardware nie mehr gewährleisten kann (außer bei hoch spezialisierter Hardware, die sehr teuer ist). Ist Hardware einmal kompromittiert, muss sie ausgetauscht werden. Das ist teuer und in vielen Fällen nicht umsetzbar.
- Hardware-Inhomogenität: Virtuelle Instanzen sind im Prinzip alle gleich, ganz im Gegensatz zu einer physischen IT-Landschaft. Das minimiert Angriffsflächen und auch cybersecurity-spezifische Aufwände durch geringere Komplexität.
- Disaster-Recovery: Wir müssen zu jedem Zeitpunkt in der Lage sein, die Funktion eines Systems wiederherzustellen. Durch den Back-up-Ansatz von Smart Data Center ist dies möglich. Damit wird der Schaden, den ein erfolgreicher Angriff verursacht, mindestens minimiert evtl. sogar irrelevant.

Was hätte die Smart Cyber Security GmbH zur Verhinderung beitragen können?

- Eines der größten Probleme in der Cybersecurity weltweit ist der Mangel an Fachpersonal, sowohl in der Entwicklung als auch in der Durchführung von Security-Audits. Smart Cyber Security wird von Anfang an den Fokus auf Automation in allen Bereichen setzen. Wir entschärfen damit den aktuellen Fachkräftemangel und bieten darüber hinaus Produkte, die sich in Zukunft beliebig skalieren lassen werden.
- Mit dem skalierbaren Produkt „Pentest Autopilot" wollen wir zuallererst das Bewusstsein dafür schaffen, dass es Schwachstellen gibt, von denen wir bisher nichts wussten (weil nicht nach ihnen gesucht wurde) und dass wir damit die Grundlage für eine Bestandsaufnahme der Ist-Situation schaffen, um dann durch weitere Dienste in Zukunft ein Mehr an Sicherheit zu generieren.
- Mit „Smart E-Mail Protect" werden wir danach unser zweites Produkt auf den Markt bringen, mit dem wir in den Bereich End-Point-Protection einsteigen, also helfen, End-Nutzer-Geräte vor Angriffen aktiv zu schützen bzw. diese von Beginn an zu unterbinden.
- Wir schaffen nach dem Prinzip von Microservices eine Architektur von Cybersecurity-Diensten und können so kontinuierlich und variabel auf Sicherheitsbedürfnisse eingehen. Durch die Verkettung mehrerer Dienste lässt sich das Sicherheitsniveau stufenweise steigern.
- Wir wollen verschiedene Bereiche der Cybersecurity abdecken und bieten damit mittelfristig eine gesamtheitliche Herangehensweise aus einer Hand an.
- In Deutschland fehlt der eine Global Player im Bereich Cybersecurity mit internationalem Format, der sich auch um den Mittelstand kümmert – der wollen wir werden und es ist zwingend notwendig, dass diese Expertise in Deutschland aufgebaut wird.

Smart Data Center GmbH
Südportal 3
22848 Norderstedt

+49 40 741 24 16 0
kontakt@smart-datacenter.de
www.smart-datacenter.de