Grüße von Lazarus

Ein vollständiger Bericht, IOCs und YARA-Regeln einer zusammenhängenden Advanced Persistent Threats (APT) Kampagne

Anatomie einer Cyberspionage-Kampagne

Das Incident Response Team der HvS-Consulting AG war an der Koordination, Analyse und Remediation mehrerer Advanced Persistent Threats (APT) gegen verschiedene europäische Kunden aus Maschinenbau und Elektroindustrie beteiligt. Die beobachteten TTPs (Tactics, Techniques & Procedures) und IOCs (Indicators of Compromise) können mit hoher Wahrscheinlichkeit der APT-Gruppe Lazarus zugeordnet werden, die vermutlich im Auftrag der nordkoreanischen Regierung aktiv ist.

Sie können hier den vollständigen Bericht (auf Englisch) herunterladen. Er enthält Details zum Verhalten der Angreifer und zum verwendeten Toolset der späteren Phasen des Mitre Att&ck Frameworks. Darüber hinaus finden Sie die identifizierten IOCs und YARA-Regeln in unserem GitHub Repository. Sie können diese gerne für Ihr Security Monitoring oder APT Threat Hunting verwenden.

Lazarus Report herunterladen →

HvS-Consulting GmbH

Parkring 20
85748 Garching bei München

Tel.: (0)89 890 63 62 - 0
E-Mail: welcome@hvs-consulting.de

© 2024 HvS-Consulting GmbH