Cybergang Silence atakuje nowe cele

ID artykułu: 57926 / 2264

URL: http://www.publikuj.org/57926

Firma Kaspersky monitoruje szkodliwe działania ugrupowania cyberprzestępczego Silence od kilku lat pierwszy publiczny raport dotyczący narzędzi i technik wykorzystywanych przez tę grupę został udostępniony jesienią 2017 r. Od tego czasu jej aktywność utrzymywała się na stałym poziomie z wyjątkiem okazjonalnych modyfikacji technik przeciwdziałających emulacji oraz wykrywaniu. Jednak na początku 2019 r. badacze z firmy Kaspersky zaobserwowali niepokojący trend: wzrost liczby atakowanych organizacji finansowych spoza regionu Wspólnoty Niepodległych Państw. W szczególności, nowe ofiary identyfikowane są w państwach regionu Azja-Pacyfik, w tym w Bangladeszu. Silence to rosyjskojęzyczne ugrupowanie cyberprzestępcze znane z atakowania organizacji finansowych. Odpowiada ono za jedne z najbardziej destrukcyjnych i złożonych operacji cyberkradzieży obok takich grup jak Metel czy Carbanak. Większość operacji tych ugrupowań wykorzystuje podobne techniki w celu uzyskania długotrwałego dostępu do sieci bankowych, a następnie monitorowania działań wewnętrznych i wykorzystania tej wiedzy do kradzieży możliwie największej ilości środków.

Silence narusza bezpieczeństwo infrastruktury swojej ofiary przy użyciu spersonalizowanych, phishingowych wiadomości e-mail. Pierwszy etap ataku wykorzystuje zatem niewiedzę lub beztroskie podejście personelu ofiary cyberprzestępcy liczą na to, że jeden z pracowników uruchomi załącznik lub kliknie odnośnik w sfałszowanym e-mailu.

W celu zabezpieczenia sieci przed potencjalnymi włamaniami badacze z firmy Kaspersky zalecają podjęcie następujących działań:

Ponieważ wiele ataków ukierunkowanych rozpoczyna się od phishingu lub innych metod socjotechniki, wprowadź szkolenie w zakresie zwiększenia świadomości bezpieczeństwa, które wyposaży pracowników w praktyczne umiejętności.

W celu zapewnienia wykrywania na poziomie punktu końcowego, badania i niezwłocznego naprawiania szkód w wyniku incydentów, stosuj rozwiązanie EDR, takie jak Kaspersky Endpoint Detection and Response.

Oprócz niezbędnej ochrony punktów końcowych stosuj rozwiązanie zabezpieczające klasy enterprise, takie jak Kaspersky Anti Targeted Attack Platform, które wykrywa zaawansowane zagrożenia na poziomie sieci na wczesnym etapie.

Zadbaj o to, aby Twój zespół z centrum operacji bezpieczeństwa posiadał dostęp do najnowszych danych dot. cyberzagrożeń, dzięki czemu będzie na bieżąco z nowymi i wyłaniającymi się narzędziami, technikami oraz taktykami wykorzystywanymi przez cyberprzestępców.

W celu zapewnienia lepszej ochrony bankomatom stosuj odpowiednie rozwiązanie zabezpieczające. Przestarzałe bankomaty, posiadające nieaktualną ochronę lub funkcjonujące bez jakichkolwiek zabezpieczeń, również wymagają rozwiązania zabezpieczającego przed współczesnymi zagrożeniami. Przykładem rozwiązania uwzględniającego specyficzne potrzeby bankomatów w zakresie ochrony jest Kaspersky Embedded System Security.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk

Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00