# 侵入の痕跡（Indicators of Compromise, IoC）

**Android に関連する IoC**

| 痕跡 | パッケージ名 | アプリ名 | C&C サーバ | 検出名 |
|---|---|---|---|---|
| 0c182b51ff1dffaa384651e478155632c6e65820322774e416be20e6d49bb8f9 | com.example.firstandoidapp | My First App | - | |
| 061b0379a12b88488db8540226e400e3f65fef9a4c1aa7744da9f17e1d93d78d | com.example.opinionpoll | OpinionPoll | - | |
| fb6ac9d93fd47db3d32f6da6320344a125e96754a94babb9d9d12b6604a42536 | com.metasploit.stage | MainActivity | https://185.225.19[.]46:4589 | AndroidOS_Metasploit.HRX |
| 468b74883536938ef3962655dfcc3ca4097ca9b5b687dfc1fef58d50e96dc248 | com.metasploit.stage | MainActivity | tcp://185.225.19.46[:]4875 | AndroidOS_Metasploit.HRX |
| a377e5f4bf461b86f938959256b7ab8b1b40bb9fd3cd45951c736a22366a8dd1 | com.example.firstandoidapp | My First App | tcp://185.225.19.46[:]4875 | AndroidOS_Metasploit.HRX |

**不正ドキュメントおよび関連するペイロードの IoC**

| 痕跡 | 脅威の形式区分 | 検体名 | **TrendX** による検出名 |
| --- | --- | --- | --- |
| 1CBEC920AFE2F978B8F84E0A4E6B757D400AEB96E8C0A221130060B196ECE010 | docx | Trojan.W97M.CVE20170199.FAIL | |
| 7238F4E5EDBE0E5A2242D8780FB58C47E7D32BF2C4F860C88C511C30675D0857 | RTF ファイル | Trojan.W97M.SIDEWINDER.A | |
| 75C158CEA14E338C8D9D32ED988C7032DA9AE6D54F5B1126ED6A83F71B9E03BF | JS ファイル「1.a」 | Trojan.JS.SIDEWINDER.A | Downloader.JS.TRX.XXJSE9EFF018 |
| AB6E8563214EEB747ABF77F9CC50796CC6A0C0562C6BEC720D7F2C978D34C412 | 偽の DUser.dll | Trojan.MSIL.SIDEWINDER.A | |
| CBD5C68F5C4345B68F018D9E5810574E8036A2BC4D826BE5C8779E8019449957 | 最終的なペイロード | Trojan.Win32.SIDEWINDER.B | |
| 34446F7F60F730FCCA145155D10D1AFF0A1153B085836DF38313772CD03C8D70 | RTF ファイル | Trojan.W97M.CVE201711882.YQUOOWV | |
| 7238F4E5EDBE0E5A2242D8780FB58C47E7D32BF2C4F860C88C511C30675D0857 | RTF ファイル | Trojan.W97M.SIDEWINDER.A | |
| AB7C1967BF1FEFDFFDE93626B78EB30994655AB02F59E0ADB0935E3E599A953F | RTF ファイル | Trojan.W97M.SIDEWINDER.A | |
| 2548A819E4C597BA5958D2D18BAA544452948E5B00271570192CCD79ABE88E8D | JS ファイル「1.a」 | Trojan.JS.SIDEWINDER.A | Downloader.JS.TRX.XXJSE9EFF018 |

| | | | |
|---|---|---|---|
| ED5E1D6E914DE64A203F2F32AB95176FC7EFFF3A520915971D5FE748E79D611C | JS ファイル「1.a」 | Trojan.JS.SIDEWINDER.A | Downloader.JS.TRX.XXJSE9EFF018 |
| 96BF8F579ACB8D9D0FF116D05FDADEF85953F11E5B2E703041FDAE0ABF5B75DC | JS ファイル「1.a」 | Trojan.JS.SIDEWINDER.A | Downloader.JS.TRX.XXJSE9EFF018 |
| 940265867D5668956D64ADF9FC4B9C6CF9E7FCFCF5C21BA7BF0BEA77B5EDD047 | 偽の DUser.dll | Trojan.MSIL.SIDEWINDER.A | |
| B22946CFEFE8646CB034F358C68CAAE5F30C1CF316CFFEAF77021C099E362C64 | 偽の DUser.dll | Trojan.MSIL.SIDEWINDER.A | |
| 89E392FA49C6A6AEB9056E3D2F38B07D0DD7AF230CD22E3B01C71F05A3AECA0B | 偽の DUser.dll | Trojan.MSIL.SIDEWINDER.A | |
| EB2D82DD0799196FCF631E15305676D737DC6E40FF588DCF123EDACD023F1C46 | 最終的なペイロード | Trojan.Win32.SIDEWINDER.B | |
| 7ECAEFCB46CDDEF1AE201B1042A62DD093594C179A6913A2DE47AB98148545DD | 最終的なペイロード | Trojan.Win32.SIDEWINDER.B | |
| 799260B992C77E2E14F2D586665C570142D8425864455CAB5F2575015CD0B87A | 最終的なペイロード | Trojan.Win32.SIDEWINDER.B | |
| brep.cdn-edu[.]net | RTF ファイルを配信する不正サーバ | | |
| www.mfa.filesrvr[.]net | RTF ファイルを配信する不正サーバ | | |

| | | |
|---|---|---|
| www.google.gov-pok[.]net | RTF ファイルを配信する不正サーバ | |
| ap-ms[.]net | C&C サーバ | |
| cdn-sop[.]net | C&C サーバ | |
| fqn-cloud[.]net | C&C サーバ | |
| ms-trace[.]net | C&C サーバ | |
| imail.aop.gov-af[.]org | フィッシングページに用いられたドメイン | |
| mail-apfgavnp.hopto[.]org | フィッシングページに用いられたドメイン | |
| mail-apfgovnp.ddns[.]net | フィッシングページに用いられたドメイン | |
| mail-kmgcom.ddns[.]net | フィッシングページに用いられたドメイン | |
| mail-mfagovcn.hopto[.]org | フィッシングページに用いられたドメイン | |
| mail-mofagovnp.hopto[.]org | フィッシングページに用いられたドメイン | |
| mail-ncporgnp.hopto[.]org | フィッシングページに用いられたドメイン | |

| | | |
|---|---|---|
| mail-nepalarmymilnp.duckdns[.]org | フィッシングページに用いられたドメイン | |
| mail-nepalgovnp.duckdns[.]org | フィッシングページに用いられたドメイン | |
| mail-nepalpolicegov.hopto[.]org | フィッシングページに用いられたドメイン | |
| mail-nepalpolicegovnp.duckdns[.]org | フィッシングページに用いられたドメイン | |
| mail-nrborg.hopto[.]org | フィッシングページに用いられたドメイン | |
| mail-nscaf.myftp[.]org | フィッシングページに用いられたドメイン | |
| mail-ntcnetnp.serveftp[.]com | フィッシングページに用いられたドメイン | |
| mail.arg.gov-af[.]org | フィッシングページに用いられたドメイン | |
| mail.moha.gov-np[.]org | フィッシングページに用いられたドメイン | |
| mail.nsc.gov-af[.]org | フィッシングページに用いられたドメイン | |

| | | |
|---|---|---|
| webmail.mohe.gov-af[.]org | フィッシングページに用いられたドメイン | |

## TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com