■ 侵入の痕跡（Indicators of Compromise、IoC）

SHA256	トレンドマイクロ製品での検出名
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	Ransom.Win32.BASTACRYPT.THDBGBB
7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a	Ransom.Win32.BASTACRYPT.YXCD2
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	Ransom.Win32.BASTACRYPT.THDBIBB
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	Ransom.Win32.BASTACRYPT.YXCD2
a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1	Ransom.Win32.BASTACRYPT.THDBGBB
1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250	Ransom.Win32.BASTACRYPT.YXCD2
2967e1d97d32605fc5ace49a10828800fbbefcc1e010f6004a9c88ef3ecdad88	Ransom.Win32.BASTACRYPT.YXCD2.note
f088e6944b2632bb7c93fa3c7ba1707914c05c00f9491e033f78a709d65d7cff	Ransom.Win32.BASTACRYPT.YXCD2.note

情報窃取型マルウェア「QAKBOT」に関連する検体：

SHA256	トレンドマイクロ製品での検出名

a48ac26aa9cdd3bc7f219a84f49201a58d545fcebf0646ae1d676c7e43c6ac3e	TrojanSpy.Win32.QAKBOT.YACEDT
82c73538322c8b90c25a99a7afc2fafcd7e7e03fe920a3331ef0003300ac10b8	TrojanSpy.Win32.QAKBOT.YACEDT
82c73538322c8b90c25a99a7afc2fafcd7e7e03fe920a3331ef0003300ac10b8	TrojanSpy.Win32.QAKBOT.YACEDT
2083e4c80ade0ac39365365d55b243dbac2a1b5c3a700aad383c110db073f2d9	TrojanSpy.Win32.QAKBOT.YACEDT
2e890fd02c3e0d85d69c698853494c1bab381c38d5272baa2a3c2bc0387684c1	TrojanSpy.Win32.QAKBOT.YACEDT
2d906ed670b24ebc3f6c54e7be5a32096058388886737b1541d793ff5d134ccb	TrojanSpy.Win32.QAKBOT.YACEDT
72fde47d3895b134784b19d664897b36ea6b9b8e19a602a0aaff5183c4ec7d24	TrojanSpy.Win32.QAKBOT.YACEDT
ffa7f0e7a2bb0edf4b7785b99aa39c96d1fe891eb6f89a65d76a57ff04ef17ab	TrojanSpy.Win32.QAKBOT.YACEDT
1e7174f3d815c12562c5c1978af6abbf2d81df16a8724d2a1cf596065f3f15a2	TrojanSpy.Win32.QAKBOT.YACEDT
130af6a91aa9ecbf70456a0bee87f947bf4ddc2d2775459e3feac563007e1aed	Trojan.Win64.QUAKNIGHTMARE.YACEJT
81a6c44682b981172cd85ee4a150ac49f838a65c3a0ed822cb07a1c19dab4af5	Ransom.Win32.BASTACRYPT.YACEDT
94428d7620fff816cb3f65595978c6abb812589861c38052d30fa3c566e32256	Ransom.Win32.BASTACRYPT.YACEDT
c9df12fbfcae3ac0894c1234e376945bc8268acdc20de72c8dd16bf1fab6bb70	Ransom.Win32.BASTACRYPT.YACEJT
0d3af630c03350935a902d0cce4dc64c5cfff8012b2ffc2f4ce5040fdec524ed	Trojan.Win32.BLACKBASTA.YXCEJ

3fe73707c2042fefe56d0f277a3c91b5c943393cf42c2a4c683867d6866116fc	Trojan.Win32.BLACKBASTA.YXCEJ
3fe73707c2042fefe56d0f277a3c91b5c943393cf42c2a4c683867d6866116fc	Trojan.Win32.BLACKBASTA.YXCEJ
0e2b951ae07183c44416ff6fa8d7b8924348701efa75dd3cb14c708537471d27	Trojan.Win32.BLACKBASTA.YXCEJ
8882186bace198be59147bcabae6643d2a7a490ad08298a4428a8e64e24907ad	Trojan.Win32.BLACKBASTA.YXCEJ
df35b45ed34eaca32cda6089acbfe638d2d1a3593d74019b6717afed90dbd5f8	Trojan.Win32.BLACKBASTA.YXCEJ
b8aa8abac2933471e4e6d91cb23e4b2b5a577a3bb9e7b88f95a4ddc91e22b2cb	TrojanSpy.VBS.KEYLOAD.A
fb3340d734c50ce77a9f463121cd3b7f70203493aa9aff304a19a8de83a2d3c9	TrojanSpy.VBS.KEYLOAD.A
5ab605b1047e098638d36a5976b00379353d84bd7e330f5778ebb71719c36878	TrojanSpy.VBS.KEYLOAD.A
9707067b4f53caf43df5759fe40e9121f832e24da5fe5236256ad0e258277d88	TrojanSpy.VBS.KEYLOAD.A
9707067b4f53caf43df5759fe40e9121f832e24da5fe5236256ad0e258277d88	TrojanSpy.VBS.KEYLOAD.A
d7580fd8cc7243b7e16fd97b7c5dea2d54bcba08c298dc2d82613bdc2bd0b4bf	TrojanSpy.VBS.KEYLOAD.A
919d1e712f4b343856cb920e4d6f5d20a7ac18d7386673ded6968c945017f5fd	TrojanSpy.VBS.KEYLOAD.A
012826db8d41ff4d28e3f312c1e6256f0647bf34249a5a6de7ecac452d32d917	TrojanSpy.VBS.KEYLOAD.A
d36a9f3005c5c24649f80722e43535e57fd96729e827cdd2c080d17c6a53a893	TrojanSpy.VBS.KEYLOAD.A

580ce8b7f5a373d5d7fbfbfef5204d18b8f9407b0c2cbf3bcae808f4d642076a	Backdoor.Win32.COROXY.YACEKT

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