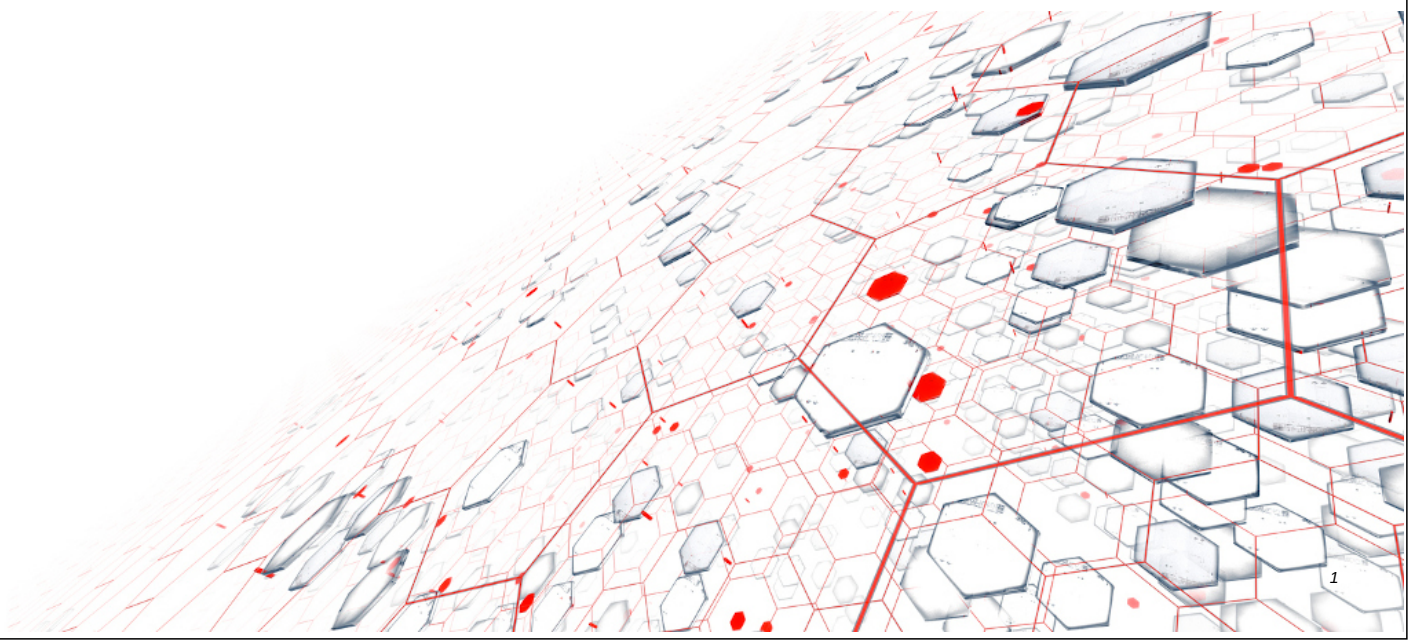
Digital Investigation of ESI

==========
Prepared by: Oxytis Forensics
==========

ACME Incorporated

==========
Date: 11 July 2022
==========



Digital Investigation of ESI

Your request to have a Digital Investigation of Electronically Stored Information (ESI) has been completed. Oxytis Forensics examined objects of digital interest made available by ACME for analysis. These objects were chosen by ACME as a representative sample of suspicious activity and/or impact of malware, or the only objects remaining of forensic interest.

Findings

Oxytis Forensics Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. ACME:

Primary findings include:

--Lorem ipsum dolor sit amet, consectetur adipiscing elit
--Lorem ipsum dolor sit amet, consectetur adipiscing elit
--Lorem ipsum dolor sit amet, consectetur adipiscing elit

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Time Zones

Oxytis Forensics follows the digital investigation standard of reporting times in Coordinated Universal Time (UTC). However, some data sources record events in local time. As a result, some of the original data presented in the disposition section of this report may be represented in local time with a time zone offset consistent with the time for your geographic region in relation to UTC. Additionally, the preferred date format is MM/dd/YYYY.

Disposition

Accounts
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Malware
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Persistence
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Exfiltration
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Manner of Compromise
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Lateral/Propagation/Replication
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Anti-forensics, Evasion & Tampering
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Remarks/Formulation
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

External Discovery

Oxytis Forensics OSINT methods attempt to discover leaked credentials and other incidental data. During OSINT we search for use of credentials in other third party services that could have minimal security protection and consequently offer an opportunity for attackers. We also look for indication of phishing services that are set up to appear to belong to coinbase.com. Oxytis Forensics attempts to find incidental or leaked documents that reside in places like pastebin, forums, search engines, and various social media sites. For example, monitoring Internet sites known to traffic information about organizational data on the dark web and open Internet could reveal active campaigns in progress.

Subdomains Registered: 4100

34-ws-feed.sandbox.exchange
qa5.developer.sandbox.exchange
a68.ws-feed.sandbox.exchange
distilleryvesper8.sandbox.exchange
public-index.sandbox.exchange
meechumlocalproxy.sandbox.exchange
ccm
jean.public.sandbox.exchange
02api.sandbox.exchange
api.learned.sandbox.exchange
pcbang.sandbox.exchange
fpdbs.sandbox.exchange
ws-feedbeastmode.sandbox.exchange
a30.sandbox.exchange
505189097486comet.papi-content-photos7.sandbox.exchange
zcash-indexer
publica74.sandbox.exchange
api-public13.sandbox.exchange
public.it.sandbox.exchange
ws-feed.obs.sandbox.exchange
pl-api.sandbox.exchange
public.de.sandbox.exchange
trial-public.sandbox.exchange
publicclient20.sandbox.exchange
avpxy01api.sandbox.exchange
...

Domains (Typosquatting): 607

Typosquatting attacks start with cybercriminals buying and registering a domain name that is either a misspelling, alternative spelling, hyphenated, or wrong domain ending .

['coinbase.sale', 'coinbase.studio', 'xn--coinba-14a98c.com', 'xn--cobase-xt7bx7b.com', 'xn--coinbse-30c.gq', 'coinbase.one', 'xn--onbase-vua3c.com', 'coinbase.works', 'coinbase.engineering', 'coinbase.com.au', 'xn--cinbase-92c.com', 'coinbase.to', 'xn--cinbase-q1a.com', 'xn--coibase-fjd.com', 'xn--coinbas-bu4c.com', 'coinbase.cyou', 'xn--coinbas-z8a.com', 'xn--conbase-veb.com', 'xn--cinbas-gva2h.com', 'xn--coinbse-9wa.com', 'xn--conbase-sfb.com', 'coinbase.trading', 'coinbase.io', 'coinbase.ir', 'coinbase.beer', 'xn--coinbas-xs4c.name', 'coinbase.net.in', 'xn--cnbase-3va9c.com', 'coinbase.re', 'xn--conbase-0ya.com', 'xn--cinbase-d5b.com', 'coinbase.exposed', 'coinbase.support', 'coinbase.ch', 'coinbase.xn--kprw13d', 'coinbase.cf', 'coinbase.om', 'coinbase.co.in', 'xn--cinbase-9mc.com', 'xn--coibase-mkb.com', 'xn--coinbae-xmd.com', 'xn--coinbas-xya.com', 'coinbase.menu', 'coinbase.plus', 'coinbase.org.ph', 'coinbase.kred', 'xn--conbas-q9a8951d.com', 'xn--coinbae-mo2c.com', 'coinbase.money', 'coinbase.si', 'coinbase.promo', 'coinbase.careers', 'xn--cinbse-lua6k.com', 'xn--coinbae-p83c.com', 'xn--cinbase-z04c.com', 'xn--conbase-8v3c.com', 'coinbase.click', 'coinbase.contact', 'xn--coinbas-xs4c.net', 'coinbase.lu', 'xn--coinbas-g9a.net', 'coinbase.company', 'coinbase.be', 'xn--coibase-6za.com', 'coinbase.com.im', 'coinbase.care', 'coinbase.gdn', 'coinbase.community', 'xn--coinbas-ov4c.com', 'xn--coinbas-9r7e.com', 'xn--conbase-pza.name', 'xn--coibase-5jb.com', 'xn--coinase-5m3c.com', 'xn--coinbas-pya.com', 'xn--coibase-2kb.com', 'xn--oinbase-15a.cc', 'xn--cinbase-khc.com', 'coinbase.today', 'coinbase.fit', 'coinbase.monster', 'xn--conbse-4va8491d.com', 'coinbase.international', 'coinbase.ag', 'coinbase.software', 'xn--cnbs-ssa3i5gvk.com', 'xn--cnbse-hwa50akj.com', 'xn--cinbase-5lb.com', 'xn--coinbse-lq4c.com', 'coinbase.limited', 'coinbase.land', 'coinbase.nz', 'xn--cinbas-gva8i.com', 'coinbase.game', 'xn--cinbase-223c.com', 'xn--coibase-o23c.com', 'xn--coinbse-ru2c.com', 'coinbase.gy', 'coinbase.vg', 'coinbase.sg', 'coinbase.fish', 'xn--coinbae-nt2c.com', 'xn--coinase-lyb.com', 'coinbase.mobi', 'xn--coinbas-ut4c.com', 'coinbase.business', 'coinbase.dev', 'xn--conbse-x1c6198c.com', 'coinbase.es', 'xn--cinbase-d5b.net', 'xn--conbase-ww4c.net', 'coinbase.ie', 'coinbase.email', 'xn--coinbas-27a.com', 'coinbase.exchange', 'xn--conbase-vgd.net', 'xn--conbase-sfb.net',

'coinbase.icu', 'xn--coinbse-30c.ml', 'xn--conbas-gva1a.com', 'xn--coinbas-z8a.xyz', 'coinbase.guide', 'coinbase.wiki', 'coinbase.tax', 'xn--coinase-4bd.net', 'xn--coinbas-j8a.net', 'xn--coinbse-t4a.com', 'xn--conbas-uva1a.com', 'coinbase.bz', 'coinbase.farm', 'xn--coinbas-z8a.info', 'coinbase.vn', 'coinbase.tc', 'coinbase.auction', 'coinbase.horse', 'coinbase.wf', 'coinbase.rocks', 'coinbase.website', 'xn--coinbas-tr3c.name', 'xn--coinase-4bd.com', 'xn--coinbae-vqb.com', 'xn--coinbse-ixa.com', 'xn--coinbas-xs4c.com', 'xn--oinbase-15a.com', 'coinbase.je', 'xn--coinbas-hya.app', 'xn--cnbase-i8a5y.com', 'xn--coinbas-w9a.com', 'coinbase.inc', 'coinbase.gifts', 'coinbase.pizza', 'coinbase.ga', 'coinbase.asia', 'xn--coinbse-30c.ga', 'xn--cinbse-zc8bxn.com', 'xn--cinbs-iwa1kvt.com', 'xn--oinbase-i6a.com', 'xn--coinbas-m1c.com', 'coinbase.li', 'coinbase.mn', 'coinbase.com.cn', 'coinbase.cat', 'xn--coibase-mn2c.com', 'xn--conbase-8ya.net', 'xn--conbase-sv3c.com', 'coinbase.tn', 'coinbase.moe', 'coinbase.pe', 'xn--cibase-3wb7879c.com', 'xn--cinbase-sx4c.com', 'xn--conbase-ww4c.com', 'xn--conbase-feb.com', 'xn--coinbse-rgc.com', 'coinbase.fr', 'xn--conbase-0ya.link', 'coinbase.cash', 'xn--conbase-8ya.online', 'xn--coinbas-hya.co', 'xn--coinbse-7o4c.com', 'xn--coinbse-4p4c.com', 'xn--coinbas-utc.com', 'coinbase.feedback', 'coinbase.com.hk', 'xn--onbase-vua5b.com', 'coinbase.chat', 'coinbase.tokyo', 'coinbase.coupons', 'xn--coibas-yt7b11b.com', 'coinbase.gratis', 'coinbase.news', 'coinbase.cafe', 'xn--cinbase-py4c.com', 'xn--cinbase-ks7e.com', 'xn--coinase-qm2c.com', 'coinbase.net.nz', 'coinbase.ovh', 'coinbase.red', 'xn--cinbse-eua4l.com', 'xn--coinbse-lwa.com', 'xn--coinbae-s73c.com', 'coinbase.fi', 'coinbase.ceo', 'xn--coinbse-9wa.site', 'coinbase.security', 'xn--cinbase-d0a.net', 'coinbase.gold', 'xn--conbse-6za74a.com', 'coinbase.mu', 'coinbase.com.my', 'coinbase.legal', 'coinbase.rs', 'xn--coinbas-et4c.com', 'xn--cobase-4va6221d.com', 'xn--cinbae-3wa09f.com', 'coinbase.tools', 'coinbase.it', 'coinbase.kz', 'coinbase.fans', 'coinbase.ma', 'coinbase.cards', 'coinbase.select', 'coinbase.ru', 'xn--coibase-6id.com', 'xn--coinbae-m93c.com', 'xn--coinbse-vn7e.com', 'xn--conbse-q9a48q.com', 'coinbase.cam', 'coinbase.casa', 'coinbase.net.ph', 'xn--coinbse-1qc.com', 'coinbase.com.ng', 'coinbase.financial', 'coinbase.wtf', 'coinbase.reviews', 'coinbase.properties', 'coinbase.pm', 'xn--coinbse-ir4c.com', 'coinbase.in', 'coinbase.sc', 'coinbase.tk', 'xn--conbase-hza.com', 'xn--oinbase-in3c.com', 'xn--coinbae-ypb.com', 'xn--coinbae-873c.com', 'xn--coinbse-twa.com', 'xn--cobase-cwa8121d.com', 'coinbase.com.tw', 'coinbase.cn', 'xn--cinbase-mz4c.com', 'xn--coibase-q4b.com', 'xn--cinbase-g43c.com', 'xn--coinbas-ru4c.com', 'xn--conbase-5tc.com', 'coinbase.cool', 'xn--coinbse-tl3c.com', 'xn--2fghl0e9ewfucwh.com', 'coinbase.management', 'coinbase.live', 'coinbase.st', 'coinbase.lol', 'coinbase.property', 'xn--oinbase-15a.cf', 'coinbase.sx', 'coinbase.party', 'coinbase.de', 'xn--cinbse-sta4l.com', 'xn--cinbase-2mb.com', 'xn--conbase-cfb.net', 'xn--coibase-jqc.com', 'xn--oinbase-l5a.com', 'coinbase.info', 'coinbase.tattoo', 'coinbase.ink', 'coinbase.institute', 'coinbase.social', 'coinbase.ec', 'coinbase.bot', 'coinbase.co.ke', 'coinbase.insure', 'coinbase.biz', 'coinbase.yoga', 'coinbase.name', 'xn--cinbase-l0a.com', 'xn--coinbas-j8a.com', 'coinbase.compare', 'xn--coinbae-m6c.com', 'coinbase.com.pe', 'xn--cinbase-1uc.com', 'xn--cinbase-mmb.com', 'xn--coinbas-wq3c.com', 'xn--cinbase-tjd.com', 'coinbase.frl', 'coinbase.tube', 'coinbase.bond', 'coinbase.co', 'coinbase.black', 'coinbase.nu', 'coinbase.site', 'coinbase.loan', 'coinbase.com.ht', 'coinbase.com.sg', 'coinbase.how', 'xn--onbase-vua1d.com', 'xn--cinbase-d0a.com', 'xn--coinbas-9r3c.com', 'coinbase.org', 'coinbase.am', 'coinbase.nom.za', 'xn--coinbse-30c.cf', 'coinbase.tw', 'coinbase.agency', 'coinbase.dog', 'coinbase.au', 'coinbase.xn--fiqs8s', 'xn--coinase-wxb.com', 'xn--conbase-9v2c.com', 'xn--coibase-b13c.com', 'xn--coinbse-op4c.com', 'coinbase.id', 'coinbase.sk', 'xn--coinbas-xya.net', 'coinbase.vip', 'coinbase.pro', 'coinbase.net', 'coinbase.la', 'coinbase.pl', 'coinbase.space', 'coinbase.video', 'coinbase.app', 'coinbase.com.ua', 'xn--coinase-pm3c.com', 'coinbase.games', 'coinbase.store', 'xn--onbase-21a3402d.com', 'coinbase.media', 'coinbase.pet', 'coinbase.fyi', 'xn--cinbase-g14c.com', 'xn--coinbas-etc.com', 'coinbase.gd', 'coinbase.ar', 'coinbase.tech', 'coinbase.love', 'coinbase.com', 'coinbase.host', 'coinbase.se', 'coinbase.finance', 'coinbase.global', 'coinbase.services', 'xn--coibase-83c.com', 'coinbase.market', 'coinbase.africa', 'coinbase.world', 'xn--conbase-8ya.com', 'xn--coinbas-z8a.tk', 'coinbase.partners', 'coinbase.science', 'coinbase.pr', 'coinbase.by', 'xn--coinbse-un4c.com', 'xn--cinbase-10a.com', 'xn--cinbase-qnc.com', 'xn--coinbas-hya.com', 'coinbase.com.mx', 'coinbase.bg', 'xn--cinbase-d24c.com', 'xn--oinbase-txa.com', 'xn--coinase-8l3c.com', 'coinbase.capital', 'coinbase.mom', 'coinbase.in.th', 'coinbase.com.co', 'xn--conbase-sfb.name', 'coinbase.xin', 'coinbase.fund', 'xn--cnbase-iwa5a.com', 'xn--oinbse-vua8991d.com', 'coinbase.london', 'coinbase.cfd', 'coinbase.onl', 'coinbase.pink', 'xn--coinbse-nkc.com', 'coinbase.org.in', 'coinbase.me.uk', 'coinbase.zone', 'coinbase.shop', 'xn--conbse-6ta3e.com', 'coinbase.mx', 'coinbase.ist', 'coinbase.team', 'xn--coinase-5m3c.net', 'xn--coinase-br2c.com', 'xn--oinbase-r5c.com', 'xn--cinbase-t2c.com', 'xn--coinbas-8xa.com', 'xn--conbase-vgd.com', 'xn--cinbase-90a.com', 'xn--cinbase-cx4c.com', 'coinbase.co.jp', 'coinbase.ind.in', 'coinbase.pk', 'xn--coinbas-z8a.net', 'coinbase.desi', 'coinbase.blog', 'coinbase.best', 'coinbase.miami', 'xn--conase-q9a5510d.com', 'coinbase.uz', 'coinbase.top', 'coinbase.academy', 'coinbase.ee', 'coinbase.build', 'coinbase.digital', 'coinbase.city', 'coinbase.casino', 'coinbase.claims', 'xn--conbse-cwa4o.com', 'coinbase.ke', 'coinbase.ng', 'coinbase.xn--ngbrx', 'coinbase.cl', 'coinbase.club', 'xn--coinbas-8jc.com', 'xn--coinbse-bo4c.com', 'coinbase.bio', 'coinbase.rest', 'xn--coinbas-g9a.com', 'coinbase.wales', 'coinbase.tv', 'xn--cinbase-2z4c.com', 'xn--cinbase-ivc.com', 'xn--coinbse-ro4c.com', 'xn--oinbase-hcd.com', 'xn--coinbas-iv2c.com', 'coinbase.solutions', 'xn--coinbas-hya.vn', 'xn--cnbase-wva9c.com', 'coinbase.art', 'xn--coibase-713c.com', 'xn--coinbas-7u4c.com', 'coinbase.co.uk', 'coinbase.events', 'coinbase.as', 'coinbase.ai', 'coinbase.nyc', 'xn--coinbse-w3a.com', 'xn--cinbase-d2c.com', 'coinbase.tel', 'coinbase.is', 'coinbase.tips', 'coinbase.at', 'xn--conbas-4va07a.com', 'coinbase.investments', 'coinbase.llc', 'coinbase.uk', 'xn--conbase-sfb.ws', 'coinbase.net.au', 'coinbase.cc', 'coinbase.page', 'xn--conbase-pza.com', 'xn--conbase-gw4c.com', 'coinbase.al', 'xn--coinbs-tta9d.com', 'xn--cinbase-urc.com', 'xn--coinbae-xxc.com', 'xn--coinbse-en4c.net', 'xn--coinbas-hya.net', 'xn--cinbase-w14c.com', 'xn--coinbas-z8a.cf', 'xn--coinbas-4v4c.com', 'xn--coinbse-fsc.com', 'xn--coibase-mkb.net', 'coinbase.ltd', 'coinbase.boston', 'xn--conbas-4va45a.com', 'coinbase.fun', 'coinbase.im', 'coinbase.link', 'xn--conbase-ydb.com', 'coinbase.af', 'coinbase.eu', 'coinbase.dk', 'coinbase.net.cn', 'xn--coinbse-30c.tk', 'coinbase.cm', 'xn--coinbse-dwa.com', 'coinbase.ro', 'coinbase.discount', 'coinbase.directory', 'coinbase.krd', 'xn--cinbase-j33c.com', 'xn--coinbse-1q4c.com', 'coinbase.com.bz', 'coinbase.group', 'coinbase.technology', 'coinbase.bet', 'coinbase.study', 'coinbase.kim', 'xn--oinbase-44a.com', 'xn--coinbse-vsc.com', 'xn--cinbase-w1c.com', 'coinbase.run', 'coinbase.cloud', 'coinbase.luxe', 'coinbase.org.uk', 'coinbase.com.es', 'coinbase.us', 'coinbase.no', 'coinbase.xyz', 'coinbase.xn--kpry57d', 'xn--coinbae-fqb.com', 'coinbase.deals', 'coinbase.fm', 'coinbase.work', 'coinbase.gift', 'coinbase.amsterdam', 'coinbase.cab', 'coinbase.ren', 'coinbase.ventures', 'xn--coibae-yt7b8i.com', 'coinbase.ht', 'xn--coinbse-fs4c.com', 'xn--cinbase-t0a.com',

'xn--coinbas-z8a.gq', 'xn--coinase-pm3c.name', 'xn--coinbs-mta5f.com', 'coinbase.surf', 'xn--cnbase-wva1c.com', 'xn--cinbas-gva8e.com', 'xn--coinbse-d4a.com', 'coinbase.sh', 'coinbase.center', 'xn--coinbae-583c.com', 'coinbase.com.bd', 'coinbase.online', 'coinbase.systems', 'coinbase.su', 'xn--conbase-muc.com', 'xn--coibase-vs2c.com', 'coinbase.com.pl', 'coinbase.cz', 'xn--coinbse-en4c.com', 'coinbase.jp', 'coinbase.wang', 'xn--cnbas-mza7nvk.com', 'coinbase.ca', 'coinbase.life', 'coinbase.hk', 'coinbase.foundation', 'coinbase.cq.cn', 'coinbase.ninja', 'xn--conbas-xva87a.com', 'coinbase.coach', 'coinbase.ge', 'coinbase.guru', 'xn--coinbse-yr4c.com', 'coinbase.report', 'xn--coinbas-dr3c.com', 'xn--coibase-rlb.com', 'coinbase.sucks', 'coinbase.expert', 'xn--coinbse-30c.com', 'xn--coibase-r13c.com', 'xn--coinbse-1wa.com', 'xn--conbase-4gc.com', 'coinbase.rip', 'xn--oinbase-44a.name', 'xn--2fgdr0ezesg4b3j.com', 'xn--coinbs-mua7a.com', 'coinbase.baby', 'xn--cinbase-8x4c.com', 'coinbase.markets', 'coinbase.credit', 'coinbase.coffee', 'coinbase.uno', 'coinbase.network', 'coinbase.loans', 'coinbase.help', 'coinbase.or.kr', 'coinbase.press', 'coinbase.training', 'coinbase.express', 'coinbase.me', 'coinbase.blue', 'coinbase.army', 'coinbase.codes', 'coinbase.gives', 'coinbase.pub', 'xn--cinbase-5y4c.com', 'coinbase.design', 'xn--coibase-b13c.net', 'xn--coinbas-gq3c.com', 'xn--coinbse-3kc.com', 'coinbase.pt', 'xn--cinbase-z33c.com', 'xn--coinbse-30c.net', 'xn--cnbase-bl8bpa.com', 'xn--oinbase-mzb.com', 'coinbase.car', 'coinbase.eco', 'coinbase.cx', 'xn--coinbas-tr3c.com', 'xn--cinbase-j04c.com', 'xn--conbase-cfb.com', 'coinbase.buzz', 'coinbase.vc', 'coinbase.camp', 'coinbase.fail']

Leaked Credentials: 2

A breach in this context is defined as an incident where data has been unintentionally exposed to the public. The Oxytis Forensics dark web monitoring and reputation management services are designed to monitor, detect and potentially suppress or remove unwanted information found on the web.

brian@coinbase.com
- Apollo
- db8151dd
- PDL
- ElasticsearchSalesLeads
- Exactis
- Gravatar
- Ledger
- NetProspex
- Playbook
- VerificationsIO
- YouveBeenScraped

amy.yin@coinbase.com
- Adapt
- Apollo
- PDL
- LinkedInScrape

Windows Forensics

The key stages of computer forensics are the use of scientific methods, collection and preservation, validation, identification, analysis and interpretation, documentation and presentation. Oxytis Forensics examines areas of the system likely to be used by malicious programs or unauthorized processes of the system that have either hijacked existing processes or created new ones.

The application, system, security and various event viewer logs are each reviewed for uncommon or illogical events and events in the timeline that are congruent with suspicious activity. These logs are a good source of information when searching for direct or consequential artifacts.

Oxytis Forensics looks for additional artifacts in the system registry of Windows operating systems that might provide context into activities during the timeline in question. Comprehensive analysis of known persistence mechanisms, software, and system configurations that reveal additional malicious software or unauthorized intrusions that typically impact these artifacts are collected.

Additionally, the following artifacts are analyzed as the registry is an excellent source for evidential data and critical during the forensic analysis process:

--Network Related Artifacts found in User and System Hives
--Volume Related artifacts found in User Hives
--Computer Metadata Related Artifacts found in User and System Hives
--Persistence Related Artifacts found in User, System, and Software Hives
--Services Related Artifacts found in System Hives
--Web Browsing Related Artifacts found in Software Hives

Oxytis Forensics also extracts components from the Application Compatibility framework that allows installed applications on a Windows box to be patched 'on the fly' (i.e. modified without a reboot), such patches can be used to spawn other processes and/or inject undesired DLLs into a patched application. This functionality offers a malware writer another way to achieve persistence across reboots.

Oxytis Forensics reviews the NTFS change log journal. The change journal is a component of NTFS that records changes made to files and is located in the $UsrJrnl MFT entry and the journal entries are in the alternate data stream $J. Useful for forensic analysis the journal records the time of change and change type.

Oxytis Forensics also recovers and examines the pagefile.sys. Microsoft Windows uses a paging file, called pagefile.sys, to store frames of memory that do not currently fit into physical memory. Windows uses the pagefile.sys file on disk as swap space, or to temporarily store some pages of memory when a system allocates more memory than will fit in physical RAM. By default, the file is never cleared.

The pagefile.sys is a random sampling of pages from RAM, without metadata about where the pages came from and processes they belong to makes any deep analysis impossible. Moreover, many kernel objects are allocated in the non-paged pool, memory regions that are never paged out to disk, and thus cannot appear in the Pagefile.

From a forensic standpoint, analyzing the $LogFile can yield a chronological list of historical transactions that were done. The $LogFile is fixed size, so once it is filled, additional data is wrapped and the old data overwritten with new transactions. Depending on the frequency of file changes made on a system the number of historical transactions will vary. To aid in this inference of time, an extrapolated timestamp from a $UsnJrnl entry or a $MFT entry is reported.

Disclaimer

Oxytis Forensics reports solely represents findings from the Exhibits made available by ACME Incorporated. Oxytis Forensics herein makes no warranties, promises, advice, nor stipulation regarding occurrences, events, or activities occurring in systems not included in scope as represented by the systems provided by ACME Incorporated.