Stop Crypto Kleptos in Their Tracks

domaintools.com/resources/blog/stop-crypto-kleptos-in-their-tracks

April 19, 2022

A Brief History of a Targeted Attack

Using tools such as DomainTools Iris Detect, Iris Investigate, and DNSDB underscore the need for cryptocurrency companies to engage with domain detection and passive DNS. Our recent research illustrates that early detection of phishing campaigns and other malicious, brand-threatening behavior are crucial as these organizations continue to gain in popularity.

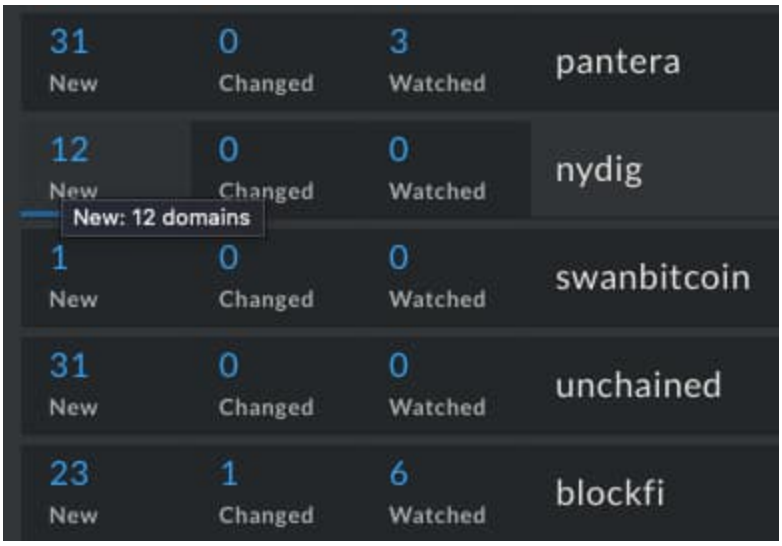
On March 18, 2022, HubSpot suffered an attack in which a bad actor accessed dozens of customer portals through an employee account. According to HubSpot this incident appeared to be a targeted harvesting attack on the contacts of cryptocurrency companies. Those companies began issuing statements, including Blockfi, Pantera Capital, Swan Bitcoin, and more.

Detection and Further Investigation Using Iris Detect and Farsight DNSDB

DomainTools has always fostered a strong culture of security expertise and awareness which continued to grow with the acquisition of Farsight Security. This includes an active and thriving discussion channel on news from the information security world, along with a desire

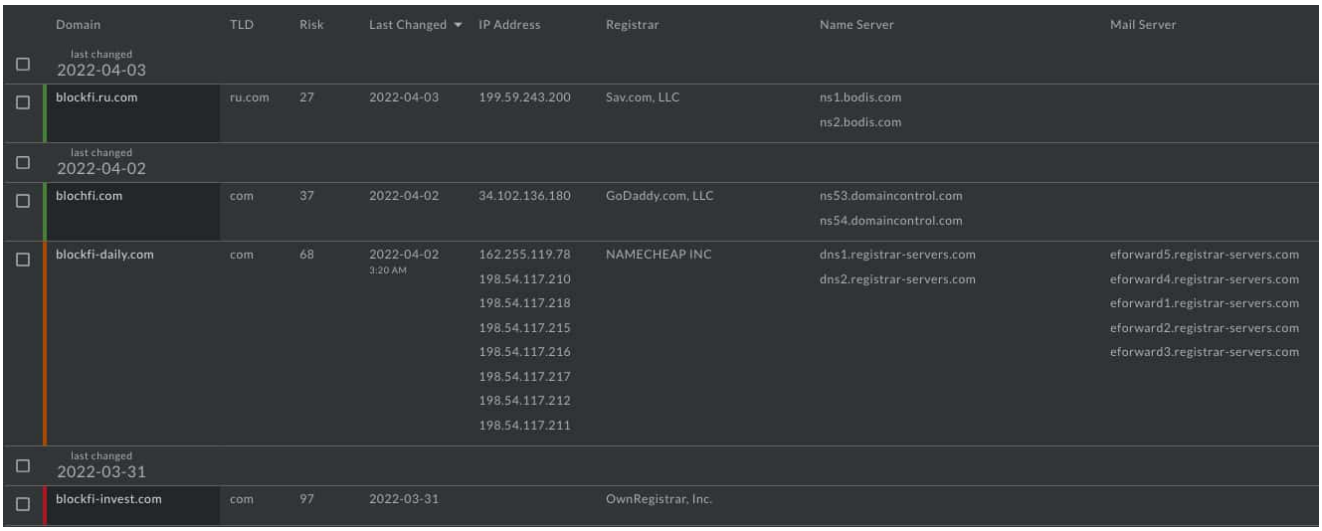
to effect positive change through what we do (such as our recent free threat-monitoring feed of newly-created Ukraine-related domains). Several of us immediately began talking about how the March 18 Hubspot breach looked tailor-made to set a malicious actor up with targets for cryptocurrency phishing campaigns. This has happened multiple times now, including Pantera Capital's HubSpot account being compromised for a fake token scam last year.

DomainTools Iris Detect is an Internet infrastructure detection, monitoring, and enforcement tool (UI and API) built on the industry's fastest and broadest domain discovery engine and the largest databases of domain data. We chose to use Detect's web browser UI in this case to show that everything involved in this kind of investigation can be accomplished in-browser, constituting a major reduction in the technical barrier-to-entry for investigative tools of this caliber. DomainTools Security Operations created a set of keyword monitors in Detect related to several of the affected companies.



A subset of domain monitors established after the HubSpot breach of March 18

A Detect search at the time showed a number of suspicious domains related to those keywords — no surprise to anyone on the internet, especially anyone working in any financial capacity. Detect allowed us to choose domains in search results to monitor closely for changes as well as to continue to see newly created domains appear as time went on. Changes tracked include hosting IP and company, registrar, nameservers, mailservers, and more.



Domain	TLD	Risk	Last Changed	IP Address	Registrar	Name Server	Mail Server
last changed 2022-04-03							
blockfi.ru.com	ru.com	27	2022-04-03	199.59.243.200	Sav.com, LLC	ns1.bodis.com ns2.bodis.com	
last changed 2022-04-02							
blochfi.com	com	37	2022-04-02	34.102.136.180	GoDaddy.com, LLC	ns53.domaincontrol.com ns54.domaincontrol.com	
blockfi-daily.com	com	68	2022-04-02 3:20 AM	162.255.119.78 198.54.117.210 198.54.117.218 198.54.117.215 198.54.117.216 198.54.117.217 198.54.117.212 198.54.117.211	NAMECHEAP INC	dns1.registrar-servers.com dns2.registrar-servers.com	eforward5.registrar-servers.com eforward4.registrar-servers.com eforward1.registrar-servers.com eforward2.registrar-servers.com eforward3.registrar-servers.com
last changed 2022-03-31							
blockfi-invest.com	com	97	2022-03-31		OwnRegistrar, Inc.		

A subset of watchlisted domains under the blockfi monitor

Fast-forward to April 3, 2022, when Trezor announced a MailChimp breach targeting cryptocurrency-related companies (having occurred on March 26). Coming so soon after the HubSpot breach, this new breach naturally piqued our interest. While malicious actors continue to be active across the Internet, they're particularly active in the cryptocurrency space. Why there? Well, as bank robber Willie Sutton once put it, "Because that's where the money is." The loose behavioral match to the March 18 breach appeared to perhaps not be "just a coincidence."

In one tweet Trezor mentioned several specific domains taken down as malicious, including xn--trzor-o51b[.]com. Sure, it looks garbled to human eyes – but this particular URL isn't yet meant for human eyes.

You see, the xn-- prefix in a URL is a technical mechanism that tells web browsers that that domain name is an IDN, or Internationalized Domain Name. Since DNS doesn't understand Unicode, domain names in other languages are represented in ASCII character form via Punycode, instead. While there are many benefits to this kind of a system, Farsight Security Co-founder and DNS expert Dr. Paul Vixie would nevertheless remind us, "Anything that can be abused will be abused." And so it is with IDN replacement. Bad actors often utilize Punycode (starting with that xn-- URL prefix) to create look-alike domains or to avoid keyword filtering

Take the above example, xn--trzor-o51b[.]com. What does that appear as in HTML-friendly email or tweets?

It displays as trẹzor. Note the special unicode character that doesn't *quite* look like an e (that tiny mark under what looks like an "e" is not just "dirt" on your screen – that's actually part of the letter!).

There are other ways to confuse recipients as well, including making the message visually busy or architecting the message with more unicode so users miss the diacritical mark. Clicking through, users expect they're going to trezor[.]com and end up at xn--trzor-o51b[.]com instead. It should be noted that malicious IDN replacement is not a new technique to fool users, and does not serve as a clear, solid indication on its own, as IDNs are used for legitimate domain internationalization.

Given this possible indicator we undertook a brief review of the previously-mentioned domain monitors set up in Detect and looked for URLs with an xn-- prefix. Two were quickly found.

```
xn--blockf-1va[.]com
xn--panteracaptal-5ib[.]com
```

What do these look like to humans when translated from punycode to unicode?

```
blockfì[.]com
panteracapítal[.]com
```

Note the diacritical mark, a confusable IDN replacement in a cryptocurrency-related domain that shows a high risk score in Detect.

This finding brought us back from the MailChimp breach to the March 18 HubSpot breach – both Blockfi and Pantera Capital were impacted in the HubSpot breach. But did more connections exist between these domains?

For that, we turn to passive DNS. DomainTools Iris cross-references multiple passive DNS sources, but we have direct access to Farsight Security's DNSDB, the world's largest DNS intelligence collection. By utilizing DNSDB Scout, we continue accessing powerful tools through a browser-based UI – an easy-to-use DNSDB interface that does not dilute the power of the tools involved.

2022-03-31 01:35:39	2022-03-31 01:35:39	1	xn--trzor-o51b.com.	xn--trzor-o51b.com.	A	62.75.175.219
2022-04-02 22:50:26*	2022-03-28 22:50:20*	6	com.	xn--trzor-o51b.com.	NS	ns1.regdom.name. ns2.regdom.name.
2022-04-05 11:03:15	2022-04-03 03:31:17	7	xn--trzor-o51b.com.	xn--trzor-o51b.com.	A	62.113.118.122
2022-04-05 11:03:15	2022-03-31 01:35:39	188	com.	xn--trzor-o51b.com.	NS	ns1.regdom.name. ns2.regdom.name.
2022-04-05 11:03:15	2022-03-31 01:35:39	127	xn--trzor-o51b.com.	xn--trzor-o51b.com.	NS	ns1.regdom.name. ns2.regdom.name.
2022-04-05 11:23:21	2022-03-31 18:09:09	136	xn--trzor-o51b.com.	xn--trzor-o51b.com.	SOA	dns37.rdn.name. root.example.com. 2022032713 10800 3600 604800 86400

An example subset of results for an RRSet query of a suspicious punycode domain through DNSDB Scout

In examining the three punycode addresses, an interesting trend emerges: after months or years of inactivity, two of the URLs became active again and the third was newly created in the last two weeks of March 2022.

```
xn--trzor-o51b[.]com - newly active as of 3/31/22
xn--panteracaptal-5ib[.]com - newly active as of 3/28/22
xn--blockf-1va[.]com - newly created as of 3/22/22
```

We now have three URLs at least matching a behavioral template by exploiting punycode, targeting the same industry (cryptocurrency), through similar mechanisms (insider/employee access), chronologically close to but related to two separate breaches of contact data (HubSpot and MailChimp), created or retrofit within nine days of each other.

One company we know was targeted for customer phishing: Trezor. Through the data above it's reasonable to infer that both Blockfi and Pantera Capital are undergoing or about to undergo phishing campaigns from the same actor. **But it is important to note that is indeed a behavioral inference, and not hard fact**.

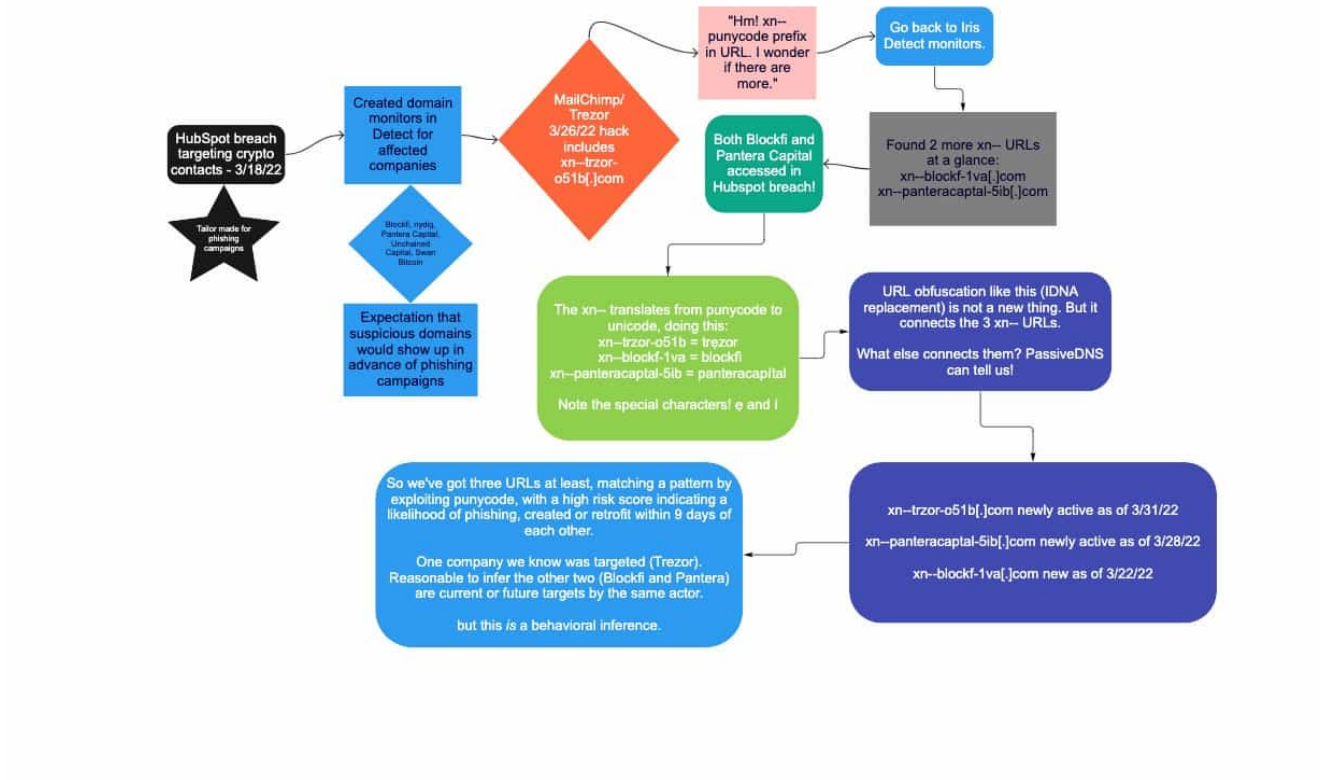
As of April 11, 2022, quite a few more IDN replacement domains popped up targeting Trezor:

```
xn--treor-kib[.]biz
xn--trezr-i91b[.]net
xn--trer-sqa53f[.]com
xn--trzr-cpa5d[.]net
xn--trzor-csa[.]org
```

While multiple suspicious domains also emerged for Blockfi and Pantera Capital, no further xn– prefixed domains have been identified. And as noted above, Detect makes it simple to continue to monitor watchlisted domains in a holistic manner – seeing possible connections as well as differences between them.

Domain	TLD	Risk	Last Changed	IP Address	Registrar	Name Server	Mail Server
xn--trezr-i91b.net *trezȯr.net*	net	53	2022-04-08	172.67.135.174 104.21.7.32	NAMECHEAP INC	bruce.ns.cloudflare.com sneh.ns.cloudflare.com	
xn--trer-sqa53f.com *trežor.com*	com	21	2022-04-08	44.227.65.245 44.227.76.166	Porkbun LLC	maceio.porkbun.com curitiba.porkbun.com fortaleza.porkbun.com salvador.porkbun.com	
trezormailer.io	io	25	2022-04-08 4:57 PM	162.255.119.98 198.54.117.218 198.54.117.211 198.54.117.216 198.54.117.217 198.54.117.215 198.54.117.212 198.54.117.210	NameCheap, Inc.	dns1.registrar-servers.com dns2.registrar-servers.com	eforward5.registrar-servers.com eforward4.registrar-servers.com eforward1.registrar-servers.com eforward2.registrar-s eforward3.registrar-s
last changed 2022-04-06							
xn--trzr-cpa5d.net *trézȯr.net*	net	21	2022-04-06	44.227.76.166 44.227.65.245	Porkbun LLC	salvador.porkbun.com curitiba.porkbun.com fortaleza.porkbun.com maceio.porkbun.com	
last changed 2022-04-05							
xn--trzor-csa.org *trézor.org*	org	63	2022-04-05		Tucows Domains Inc.	2-can.njalla.in 1-you.njalla.no 3-get.njalla.fo	

A subset of watchlisted domains within a Trezor monitor in Iris Detect



Recommendations

Given multiple recent breaches all targeting the cryptocurrency industry, cryptocurrency-related companies should immediately “step up their game.” Employ domain detection and passive DNS solutions to protect your brands and to detect suspicious domains and possible phishing campaign infrastructure before a campaign against your company begins in earnest.

Newly created or newly-active IDN-replacement domains with high risk scores, among other available indicators, can warn companies of imminent phishing or other imminent malicious campaigns and allow them to preemptively request takedowns or perform other preventative keyword monitoring, and regular expression and expandname features make complicated queries easier.

Expandname and regex also allow security partners or other researchers to more easily search passive DNS for pattern-matching results. These results need not be specific to a particular brand or keyword in order to identify ongoing or upcoming malicious activity campaigns. As another example of this, consider the domain-generating algorithm involved in SUNBURST and Farsight’s related report.

Download Now

Cookie	Duration	Description
cookielawinfo-checkbox-analytics	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookie is used to store the user consent for the cookies in the category "Analytics".
cookielawinfo-checkbox-functional	11 months	The cookie is set by GDPR cookie consent to record the user consent for the cookies in the category "Functional".
cookielawinfo-checkbox-necessary	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookies is used to store the user consent for the cookies in the category "Necessary".
cookielawinfo-checkbox-others	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookie is used to store the user consent for the cookies in the category "Other.
cookielawinfo-checkbox-performance	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookie is used to store the user consent for the cookies in the category "Performance".
viewed_cookie_policy	11 months	The cookie is set by the GDPR Cookie Consent plugin and is used to store whether or not user has consented to the use of cookies. It does not store any personal data.

Functional cookies help to perform certain functionalities like sharing the content of the website on social media platforms, collect feedbacks, and other third-party features.

Performance cookies are used to understand and analyze the key performance indexes of the website which helps in delivering a better user experience for the visitors.

Analytical cookies are used to understand how visitors interact with the website. These cookies help provide information on metrics the number of visitors, bounce rate, traffic source, etc.

Advertisement cookies are used to provide visitors with relevant ads and marketing campaigns. These cookies track visitors across websites and collect information to provide customized ads.

Other uncategorized cookies are those that are being analyzed and have not been classified into a category as yet.