Make Crypto Assets First-Class Citizens in Threat Intelligence

Chris R. Adams

As the world evolves from Web 2.0 to Web 3.0 - think decentralized protocols for crypto assets, identities, and compute-services leveraging blockchain technology - cyber threat teams must evolve their understanding of the technology at play to stay ahead of threats. That's easier said than done. Some of the challenges that security teams face are learning Web 3.0 terminology, understanding new threat vectors involving Web 3.0 technology, and a lack of support from existing toolsets to help analyze such threats.

This blog will highlight how crypto assets are used in cybercrimes, what specific threat indicators to look out for, and how to apply the Diamond Model for Intrusion Analysis to a specific threat involving crypto wallet addresses within ThreatConnect's Threat Intelligence platform. Lastly, I introduce how ThreatConnect helps manage this threat data and scale the process of finding relevant context around crypto assets using 3rd party enrichment services.

The New Money

It's been stated that criminals prefer crypto assets over traditional fiat currencies, and because of that, crypto-assets like Bitcoin should not be adopted. That argument never made sense to me since one can track asset wallet addresses activity and transactions much more easily and quickly than US dollars flowing across boundaries and bank accounts. Either way, the trend for cybercriminals to demand crypto assets over fiat currency is increasing.

In his Financial Cybercrime article, John Hammond describes how criminals obtain crypto assets:

- **Ransomware** - the intent is to hold ransom by encrypting a user's information and making them pay in crypto assets for it to be decrypted
- **Data Exfiltration -** critical data is stolen and will only be returned or destroyed upon being paid in crypto assets
- **Crypto mining -** Leverage a victim's infrastructure for mining cryptocurrencies where the criminal receives crypto assets as payment (Cryptojacking)

The US Government is obviously taking notice of crypto assets (referred to as virtual currencies) being used for criminal activity and acting upon it. The Financial Crimes Enforcement Network (U.S. Treasury Dept.) recently listed "cybercrime, including relevant cybersecurity and virtual currency considerations" as a national priority. This means security teams should expect those involved in criminal investigations and forensics to want details and a systematic means to track related threat data to support criminal cases. Threat intelligence systems of record, tools, and analysis methodologies should support crypto assets fully so those details can be stored and managed like all other cyber threat intelligence.

Crypto Asset Indicators

Let’s now consider some examples of crypto assets and what might be considered threat intelligence indicators. The reality is crypto assets have traditionally been treated like 2nd or 3rd class citizens, which implies they play a background role as a note or an attribute - not a full-fledged supported object or entity.

This blog post from Loginsoft does a great job describing the need for crypto asset support in Threat Intelligence Platforms, like ThreatConnect. Some key Threat Intelligence objects or activities mentioned were:

- Crypto asset address details and related risk (i.e., illicit or criminal history associated with a Crypto assets address)
- Crypto asset wallet owners and their location
- Transaction history (inbound and outbound)
- Transaction risk (risk-based upon transaction characteristics, i.e., illegal dark web activity, etc.)

The data set that characterizes typical threat actor behavior, activity, and weaponry certainly carries over from traditional cyber threat intelligence where analysts are interested in cryptographic keys, file hashes, URLs, malware, IP addresses, hosts and domains, etc. But we need to accommodate for some of these new threat indicators in our system of record.

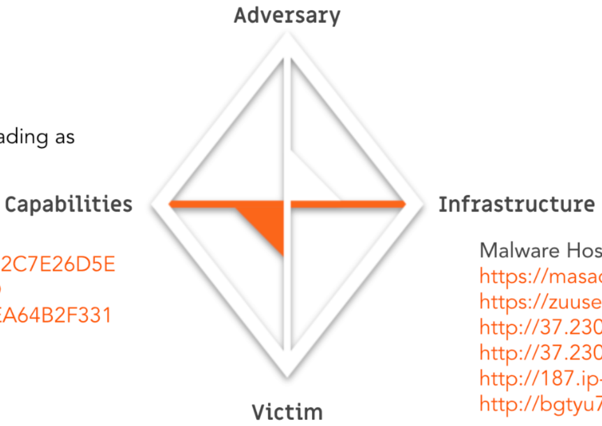
Before we dig into the details of how to do that, let’s look at what we’d want a threat data model to include.

A Diamond Model for Diamond Hands

The Diamond Model for Intrusion Analysis Framework helps analysts think through piecing together the most critical elements of an intrusion and uncover holes in infrastructure or exploitation tactics; it also helps capture trends in terms of what actors do in hopes of prevention in the future.

As an example of building out a model in a TIP platform like ThreatConnect, I referenced this post about the Masad Stealer spyware in Peter Zacherginsky's blockthreat.io, which is one of my go-to references for blockchain-related threat intelligence. Items related to the threat are mapped to specific vertices in the diamond: Adversary, Capabilities, Infrastructure, and Victim, as seen in the graphic.

Bitcoin Wallet Address:
1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe
Monero Wallet Address
42Mm9gjuUSmPNr7aF1ZbQC6dcTeSi1MgB1Tv41frv1ZRFWLn4
wNoLH3LDAGn9Fg2dhJW2VRHTz8Fo9ZAit951D2pDY8ggCR



Masad Stealer
- Trojan-delivered malware, masquerading as
legit third party Windows tools

SHA-256 Malware file indicators
1ACF5A461EE16336EB8BBF8D29982C7E26D5E
11827C58CA01ADAC671A28B52AD
0DCF547BD8F4074AF97416D8B84EA64B2F331
9064AA4BCE64AD0C2E2D3957175

Malware Hosting and C2
https://masadsasad.moy.su/base.txt (miner)
https://zuuse.000webhostapp.com/mi.exe (miner)
http://37.230.210.84/still/Build.exe
http://37.230.210.84/still/SoranoMiner.exe
http://187.ip-54-36-162.eu/steal.exe
http://bgtyu73.ru/22/Build.exe

Client Desktops
Cryptocurrency Wallets
Credit Card Browser Data
Browser passwords & Cookies
Desktop Files
AutoFill browser fields

The threat actor uses capabilities (malware) to perform an attack and leverages infrastructure to host (malware) or operate (C2), causing pain to the victim. Indicators to be on the watch for include malware file hashes and URLs or IP Addresses where the malware may be hosted or where command and control may be performed from, respectively. Those indicator types are generally well supported in TIP platforms such as ThreatConnect.

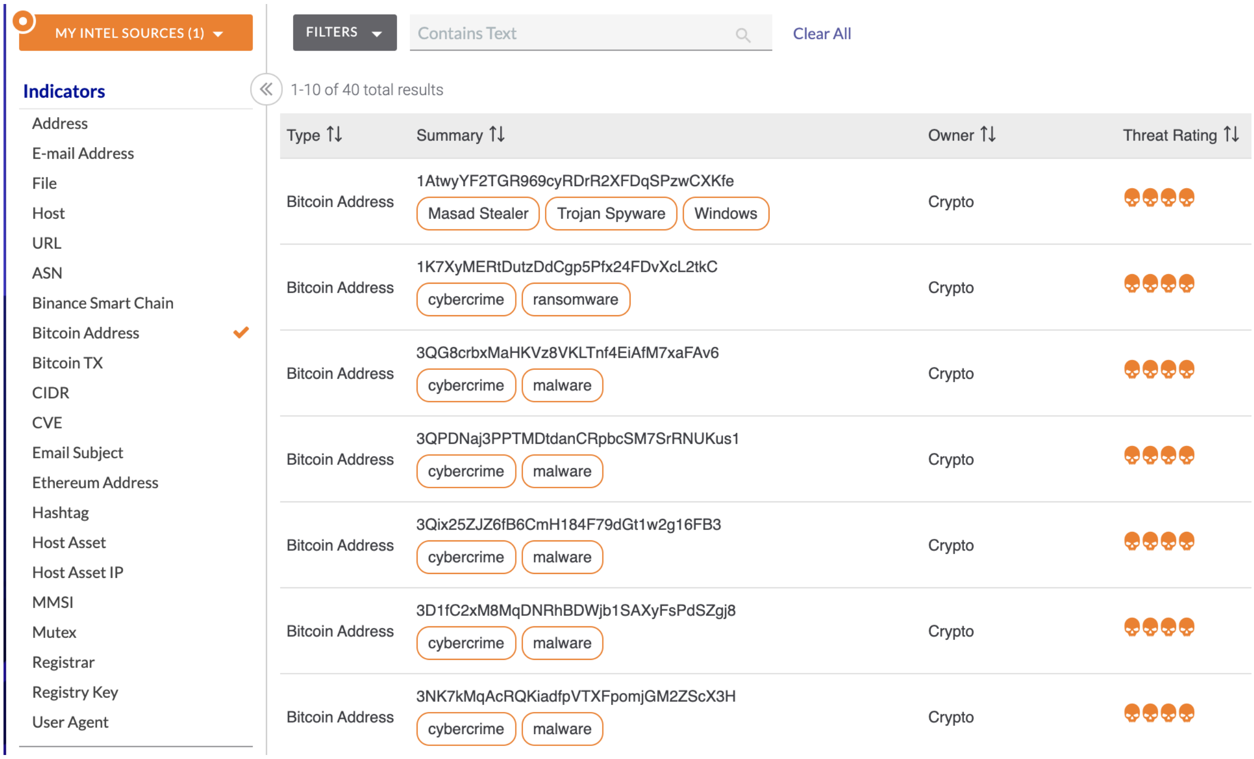
However, wallet address indicators such as Bitcoin or Monero are not natively supported, so I created custom indicator types for each of those. Creating a custom indicator is straightforward in ThreatConnect. You simply define the Regular Expression (Regex) to ensure the system can identify the unique characteristics of the string. Here is what I've used for the Bitcoin Address:

Bitcoin Address \b([13][a-km-zA-HJ-NP-Z1-9]{25,34})\b

Perhaps you can tell that this expression forces the first character in the address to be a 1 or a 3, which is the rule for Bitcoin addresses, or it will be ignored.

Now that I've defined the indicator type, I can load Bitcoin addresses at will and associate them to other threat group types or indicators. ThreatConnect also provides a native API endpoint for each custom indicator so that I can write or read them in bulk which will come in handy should **blockthreat.io** begin to serve wallet addresses and other crypto asset indicators via API.

Here is a screenshot of some Bitcoin address indicators that have been loaded and can now be treated as first-class citizens in the platform.

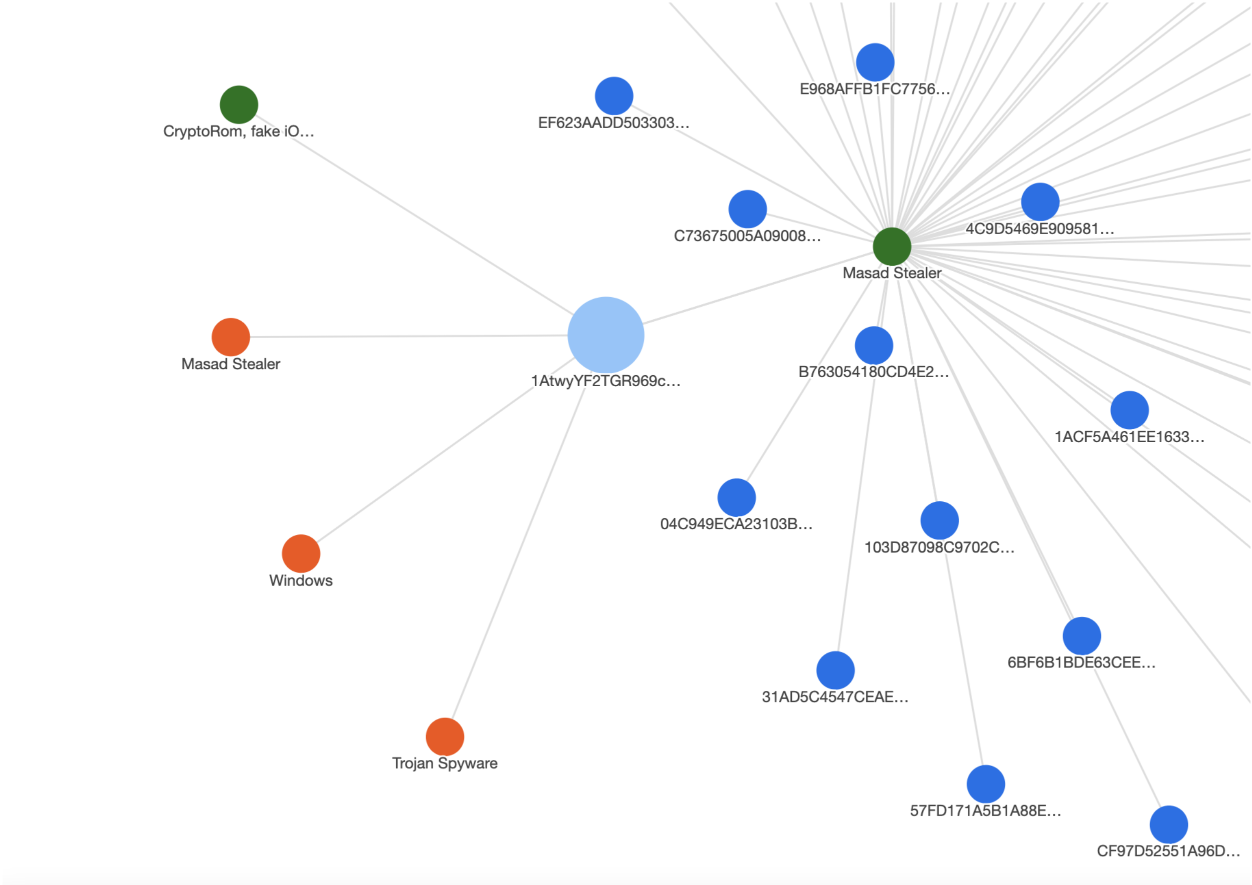


1-10 of 40 total results

Type ⇅	Summary ⇅	Owner ⇅	Threat Rating ⇅
Bitcoin Address	1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe Masad Stealer, Trojan Spyware, Windows	Crypto	💀💀💀💀
Bitcoin Address	1K7XyMERtDutzDdCgp5Pfx24FDvXcL2tkC cybercrime, ransomware	Crypto	💀💀💀💀
Bitcoin Address	3QG8crbxMaHKVz8VKLTnf4EiAfM7xaFAv6 cybercrime, malware	Crypto	💀💀💀💀
Bitcoin Address	3QPDNaj3PPTMDtdanCRpbcSM7SrRNUKus1 cybercrime, malware	Crypto	💀💀💀💀
Bitcoin Address	3Qix25ZJZ6fB6CmH184F79dGt1w2g16FB3 cybercrime, malware	Crypto	💀💀💀💀
Bitcoin Address	3D1fC2xM8MqDNRhBDWjb1SAXyFsPdSZgj8 cybercrime, malware	Crypto	💀💀💀💀
Bitcoin Address	3NK7kMqAcRQKiadfpVTXFpomjGM2ZScX3H cybercrime, malware	Crypto	💀💀💀💀

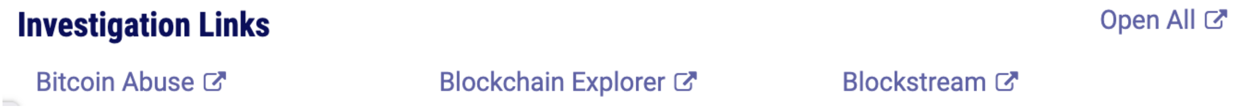
As you can see under **Indicators** on the left, I've also added Bitcoin Transactions, Binance Smart Chain, and Ethereum as other indicator types.

One of the benefits of building a model and aggregating data over time is that when pivoting through it, one will discover new associations or relationships that otherwise may have gone unnoticed. ThreatConnect helps visualize these relationships with a simple click, as presented in the image below.



Notice the association between Bitcoin wallet 1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe and the Masad Stealer family of file hashes - this is where we see the diamond model structured earlier come to life. We also now see that same wallet associated with the CryptoRom, fake iOS malware attack. This is shown for illustration purposes only, but the point is that as cases grow over time, analysts will be able to determine when the same wallet is used in multiple incidents.

Lastly, one of the critical functions that analysts need to perform to gain context about indicators is to automate the search for information pertaining to the address. Investigation Links can easily be configured within the details page of the indicator, and here are a few I've set up for Bitcoin Addresses. Click on these links, and the Bitcoin wallet address is passed as an argument to the website, and the page loads in a separate tab with the response for that particular indicator which comes in handy for quick analysis.



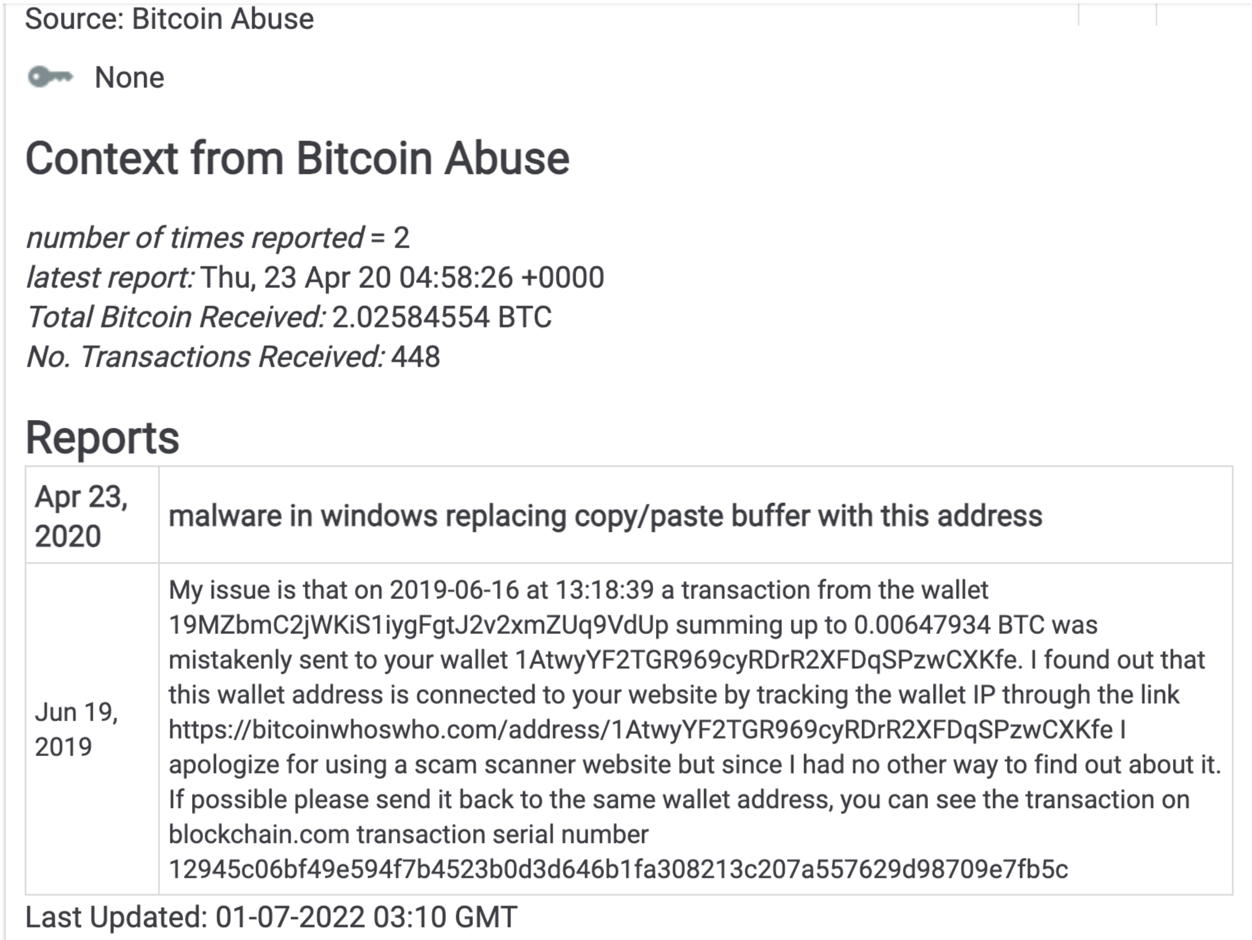
Investigation Links

Open All

Bitcoin Abuse   Blockchain Explorer   Blockstream

This is a good start; however, what if you want to enrich hundreds of thousands of wallet addresses? This is where scaling with automation can save analysts massive amounts of time. ThreatConnect introduced playbooks for this very reason.

A playbook queries the 3rd party enrichment service API (Bitcoin Abuse) and parses the results storing pertinent information as attributes (and applying markdown). While a walkthrough of building that out with playbooks is beyond the scope of this blog, here is an example of enrichment data collected from Bitcoin Abuse and stored within our wallet indicator's source attribute pinned to the Bitcoin address in ThreatConnect.



Source: Bitcoin Abuse

None

Context from Bitcoin Abuse

number of times reported = 2
latest report: Thu, 23 Apr 20 04:58:26 +0000
Total Bitcoin Received: 2.02584554 BTC
No. Transactions Received: 448

Reports

Apr 23, 2020	malware in windows replacing copy/paste buffer with this address
Jun 19, 2019	My issue is that on 2019-06-16 at 13:18:39 a transaction from the wallet 19MZbmC2jWKiS1iygFgtJ2v2xmZUq9VdUp summing up to 0.00647934 BTC was mistakenly sent to your wallet 1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe. I found out that this wallet address is connected to your website by tracking the wallet IP through the link https://bitcoinwhoswho.com/address/1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe I apologize for using a scam scanner website but since I had no other way to find out about it. If possible please send it back to the same wallet address, you can see the transaction on blockchain.com transaction serial number 12945c06bf49e594f7b4523b0d3d646b1fa308213c207a557629d98709e7fb5c

Last Updated: 01-07-2022 03:10 GMT

The value here is that analysts don't need to spend days, if not weeks looking up context related to addresses. They can scale that process by leveraging automation and begin to include data from multiple 3rd party sources.

In summary, with ThreatConnect treating crypto assets as first-class citizens, they become a primary object within the threat data model. With API access, they can be part of larger bulk processes when the need comes. And it will. What I've shown in this blog should help security teams get ahead with storing and managing crypto assets that are used in incidents or related to threat vectors currently being monitored. In a future blog, I’ll provide more detail on how playbooks can provide automated enrichments against various services.